University of
South Wales
Prifysgol
De Cymru

An Investigation Into How Engaged People Are In Online Privacy Issues, Are They Aware Of Their Rights, How Data Is Taken, And How To Prevent It.

Ieuan Paynter 16651243

Supervisor: Andrew Bellamy

Statement of Originality:

IS3D660 and IY3D660 Individual Project

This is to certify that, except where specific reference is made, the work described within this project is the result of the investigation carried out by myself, and that neither this project, nor any part of it, has been submitted in candidature for any other award other than this being presently studied.

Any material taken from published texts or computerized sources have been fully referenced, and I fully realize the consequences of plagiarizing any of these sources.

- Student Name: Ieuan Paynter
- Student Signature: I._Paynter
- Registered Course of Study: Cyber Security
- Date of Signing: 07.06.21

Acknowledgements:

I would like to thank all the cyber security staff at USW, they have all been great lecturers during my time at the university. Time spent on campus was cut by a full year, but I have still had support from lecturers and my friends I have made while studying at the university over three years. It may not have been the final year that I wanted, and a lot of things have not been able to go to plan, but I can say that I have completed three years at the uni and left a better person. I would like to personally thank Peter Eden and Andrew Bellamy. Both have been incredibly supportive, and offered guidance when I needed it. You have both been wonderful and engaging lecturers during my time at USW, thank you both for all the help and the hard work you put into teaching students, especially during the Coronavirus pandemic.

I would also like to thanks my family; they have helped me immensely through my time at USW, especially during the pandemic and the writing of this report. The support from my grampa, sister and my mother has allowed me to write this dissertation while dealing with the stress of the pandemic, relationship issues, and the serious personal health issues I have experienced this year. Without them my time at university, especially in year three would have been a lot harder, I cannot thank them enough.

Abstract:

Today's world is always online, including our data. So it is important to know where this data is going, how it's being used, who is collecting it, and how it is being collected. This dissertation is written to research how our day to day lives are affected by online data collection, and the nefarious reasons it is used against us. The report will explain these issues, its effects on society, our digital rights, and how to prevent it in an easy to understand, nuanced way explaining both sides of this argument.

Contents

Chapter 1 – Introduction:

This report was written for a number of different reasons; however, the main reason is due to the fact that today's ever growing online world has all of us connected to each other like never before. This level of connection has made it so that almost all aspects of our lives has been digitally preserved online, and is still being added to everyday. This online preservation of our interests, connections, purchases, and locations, can be used in many different ways, some good and some bad. This report goes into this topic, covers a wide range of opinions, and provides a nuanced and fairly straightforward explanation of how and why this data is being collected and by whom. With the recent controversy of people such as Edward Snowden, or Julian Assange bringing awareness to the public of what is happening with user data, this report is important as it is a method that lets the everyday person have a fairly simple and nuanced way of learning about this topic.

1.2: Aims and Objectives:

People know how to protect against general day to day viruses etc., they don't know how to protect their own data from companies, government spying. This report aims to explain what consumer's digital rights are; different methods of protecting their data in a simple nuanced way, and create a guide that covers all of the different but important issues that will be looked at within this topic. Another aim of this report is to leave the reader feeling informed enough so that they can form their own opinions, come to their own conclusions using the evidence in my report, and then decide what is best for them to do using the guide.

This will be done in a number of ways, such as; looking at and using good sources of information that are fair, and cover all sides of the digital privacy debate. The report features a survey that was given to the public and answered anonymously. This survey includes questions such as; do you consider yourself well-informed on the topic of on-line privacy, and the rights you have on-line?", "do you trust large companies to take care of any data they may have on you?", "have you ever been effected by a data leak?" This report also aims to further my own understanding of how data is gathered, and what it is used for.

1.3: Research Objective:

The objective of this project is to raise awareness and help people with little or no understanding on the complicated issue of on-line privacy and digital rights. Readers will gain an understanding of the matter that they can then use to make informed decisions about their on-line privacy, and make then make changes with the help of a guide.

Chapter 2 – Literature Review:

Before writing a report research must be done on other guides and reports online, so that they can be compared, and an idea of where "gaps in the market" can be filled. Conducting this research gives a better understanding of what was already out there, what works and what doesn't. While doing this research I have tried to find sources that are not biased to particular viewpoints, recommend solutions in their own self-interest, and that they are from authentic sources of integrity. While conducting this research I found that this was a gap in the market. You can find many different guides to privacy all over the internet, however they are not always fair, nuanced, and make use of genuine sources of information. To conduct these literature reviews, I made use of the CRAAP test (Currency, relevance, authority, accuracy, purpose) methodology. This method is used to test the reliability and overall usefulness of a source. I have chosen to review sources that cover key points in my report, so that I can fill any missing gaps, streamline the available knowledge, and produce my guide.

Source one: User privacy – A practical guide for librarians:

(Connolly, 2018)

Overview:

This online privacy guide, written for librarians firstly covers the “privacy landscape” in modern society in the context of a library setting. This short introduction introduces the reader to the problems the book covers, and gives a short summary of the privacy issues, laws and moral duties a modern library faces. The introduction is a well written and brief one that covers the state of things, and tells the user what the book is going to cover before introducing the next chapter on malicious hackers.

Layout:

The guide has a very academic layout; this makes it a very good source for information as this type of layout is a good way to convey lots of information in a professional manner. However, as my guide is planned to be easily accessible in terms of its ability to be picked up, read and understood easily by those of differing technical knowledge, this method of conveying the information in a guide is far too rigorous for my plan and wouldn’t meet the objectives. What I can take from this source is the method in which the guide has been written with its target audience I mind. The guide is “written to help librarians and library workers buttress their own privacy protections and help their users to do the same.” *(Connolly, 2018)* Those who work in a library will need to have a high reading comprehension level, and while given lots of technical terms in a very academic method, will still be able to digest the information and make use of it. For my guide I had to make sure that it was written with my target audience in mind, and that I met my objectives of being clear, concise, easy to understand, nuanced, and unbiased.

Currency:

This source was written in and published in 2018. I could not find and updated or revised editions of this book, nevertheless, the information in the book remains fairly relevant as the same issues on privacy covered in the book are still talked about in 2021, and may in fact looking at my primary research and the results I got, actually be more relevant as the topic is becoming more and more relevant in society. The techniques used for privacy that the book suggest such as the use of correct passwords styles, or limiting the information uploaded to social media accounts are still relevant techniques used in 2021 to increase online privacy.

Relevance:

This source is relevant to my topic for a number of obvious reasons. Firstly, the book is a guide to online privacy, as is mine. This source is also relevant because it clearly states who its target audience is and meets it. This is relevant to me as my target audience was quite vague. My target audience was the everyday person that isn’t well informed on the subject. This source showed me how to convey information to a target audience without going off topic.

Authority:

The author of this book, Matthew Connolly is clearly an author that researched the topic of this book well. The information in the book is both correct, and relevant, as previously stated. Matthew is an application and web developer at Cornell university library, and has worked there for over 10 years. Being in this position for that long, and having written many articles, books, and journals he is a good source as he is clearly well qualified. The publisher, Rowman & Littlefield are an American independent publishing group that originated in 1949. The publisher is a good source of authority as they are both successful, and have many awards such as having 22 titles awarded the prestigious honour on 2020. *(Rowman & Littlefield, 2020)*

Accuracy:

All the information in the book is sourced from relevant places and referenced at the end of the end of each chapter as well as the end of the book. As stated above the content of this book is both relevant and current in 2021. The author as well as the publisher is experienced. Therefore the sources used are accurate. The referencing style is also very similar to the Harvard style I have used in this report.

Purpose:

Similar to my report and guide, this source is a book written to guide readers on their online privacy. The book is written for librarians so that they know their own privacy rights, and those of their patrons. The guide informs the reader of the issues faced today and how to best combat them, and prepare a library to deal with the topic. The purpose of the book is clearly stated in the preface section and also features an assumptions section. This section covers the meanings of specific and important topics the book covers such as "privacy, and security".

Overall I think this source is good to use as a reference and guide when writing for a number of reasons. Firstly, the topic of online privacy is the same as my guide, although this book is focused on libraries, it still covers the basics of online privacy. This is also stated in the preface section of the book "However, there is enough general information about privacy threats and countermeasures in this book to serves a wider audience". I used this book as almost a source of inspiration and as guide for writing guides on this topic. The source knows its target audience well, has written it for them well, and uses relevant information.

Source two: The effect of online privacy policy in consumer privacy concern and trust

(Editorial board - Science Direct, 2012)

Overview:

This source is a scholarly journal that is "dedicated to examining the use of computers from a psychological perspective." The journal is written by multiple editors on an editorial board and covers the same topic as my report. This source uses multiple methods of research such as, literature reviews, surveys, and other journal articles and presents this information in the report along with the use of tables. This journal was very beneficial for my work as it covers a similar topic, however this is a much more scientific and technical report than my own or the previous source I listed. This journal gave me a better understanding of how to present the information and evidence that I had found during my research.

Layout:

The layout of this source is very similar to my own layout. It features an abstract, introduction, a literature review, and then gets into the main body of writing before finishing with a conclusion. This layout is very professional and what I think is the best way to frame a report that uses lots of evidence and tables to support its points.

Currency:

The journal article was written and published in May of 2012; this is a few years before big privacy controversies such as Cambridge analytica, or the Edward Snowden NSA leaks. However, based on the techniques covered and the research they have conducted, this report is still relevant in 2021. The report is part of an online journal called Computers in Human Behaviour, which was last updated in September of this year. All the links to the sources used are still functional but I don't think this is as relevant as it could be if it was updated along with the rest of the journal. This report however, uses lots of primary research they have conducted and is therefore current to its own research.

Relevance:

As stated above this report was written in 2012 so it is not as relevant as other sources out there. However, the information used by the authors is still correct, relevant in terms of online privacy and how internet users feel both before recent controversies, and after as it gives extra insight when read now. This report is relevant to me for the reasons already given, but also because it shares a common topic, methods of research (the authors and myself both used surveys), and both talk about the positive and negative effects of internet globalisation.

Authority:

This journal article is from a larger internet article called "Computers in Human Behaviour" written by multiple authors on an editorial board on behalf of Science Direct. The authors on the board are all highly skilled writers with high level degrees in a wide range of fields that relate to this topic. The journal article has also been citied 160 times by others of various authorities' right up to the present year. This also backs up the point that the information used is still relevant. Science Direct is an "online bibliographic database of scientific and medical publications". It features many different types of journals, books, and articles from leading scientific sources all over the world. Science Direct is owned by Elsevier a huge publisher and with them has 18 million articles and chapters, and 2,500 peer-reviewed journals. *(Wikipedia, 2021) (ScienceDirect, 2021)*

Accuracy:

The information used in the article comes from many different reputable sources chosen by the highly educated authors on the board of directors. As stated above Science Direct is a massive online bibliography database that has 18 million articles and chapters, and 2,500 peer-reviewed journals. This means that all the information used on their site must be accurate and from reliant sources.

Purpose:

The articles purpose "aims to investigate trust and privacy concerns related to the willingness to provide personal information online under the influence of cross-cultural effects." *(ScienceDirect, 2021)* As this is a very similar topic to my report and guide, I have chosen to use this as source for similar reasons as the first source. This article is highly articulate, uses technical terms but does a relatively good job at covering the topic in an easy to understand manner. My objective was to create a report that covers this topic, but is easily understood by the public, is not nuanced, and the guide can easily be followed by those who are not as technologically literate, while also being useful to those with more skill in the field.

Source three: The beginners guide to online privacy

(Gulea, 2018)

Overview: This source is a beginner's guide to online privacy as is stated in the title. It is created by freecodecamp.org, which is an educational organisation that offers free courses in different programming languages online. This guide, while it features all the information one could need to monitor their online privacy, only makes use of mass amounts of text and very little images. This method of producing a guide only suits those whose learning style is reading. The guide is also not suited for those that would like to get key points of information quickly on a webpage that is easy to use and navigate efficiently.

Layout:

As stated above the layout of this guide is not very user friendly, the guide is just a wall of text with a few images sparsely placed throughout. This guide also has no references section for the reader to look at the information sources themselves. It does however feature a 'useful links' section that provides readers with some links to privacy tools such as, weekly hardware reports, or browser safety checkers. This is good as it means readers can stay up to date with their online privacy and be proactive.

Currency:

This article was written in January of 2018 so it is not a source that was currently written. This however, does not mean that the information in the guide is not still current as some of the topics covered such as; why should one care about their privacy, alternatives to the popular devices/tools.

Relevance:

This article was written in 2018, however the information used and the advice given are still current. As stated above, the guide is still relevant current year as it covers many topics that are, if anything becoming more and more important as time goes on. This source is relevant because it is also a guide to online privacy like the one developed for this project. This guide is a good source of inspiration, ideas for where gaps can be filled, and a point of comparison.

Authority:

This guide was produced by free code camp. A non-profit, online-educational organisation, that was founded in 2014 by Quincy Larson. The organisation was set up in order to provide an updated model of learning how to program, for free and online. The organisation, while not a renowned one, is used by 350,000 users a month (Larson, 2017), and is used alongside traditional education establishments such as schools, colleges and universities, is trusted globally.

Purpose:

The purpose of this guide is to inform the reader of the different topics covering online privacy, so that they can make an informed decision on their privacy, and review how they use the internet, and what the reader puts out there. The purpose to this guide is very similar to the one in this project.

Source four: Online Privacy: 11 Ways to protect yourself in 2021(and beyond)

(Rembert, 2021)

Overview:

This source is another report that that gives readers advice on how to safeguard their online privacy. As with the previous source, this one also covers all the topics a reader will need to make more informed decisions on their privacy. This “ultimate online privacy guide” as the page is titled, provides the reader with the different methods one can take to prioritise their privacy when online.

Layout:

The layout of this page is very simple; it features different sections of text, accompanied by images. It is clear to see when compared to the previous source that just had walls of text and a few sparingly used images, that the layout used here is a more user-friendly one. The information used is more straightforward and kept brief so that the reader absorbs key information that isn’t bloated with jargon or technical language that some readers may be not understand.

Currency:

This page was last updated in January 2021 and, as with the previous sources covers topics that are still relevant and will therefore need to use points that are current. The advice given is still current and seen in other guides to privacy such as the previous source covered. The guide also states that it lists “11 ways to protect yourself in 2021 and beyond” this along with what is already covered shows that this guide is indeed relevant now, and for the foreseeable future.

Relevance:

This source is a guide to online privacy and how readers can protect themselves while using the internet. This source is therefore relevant to this project as it covers the same topic, is a guide with a ‘reader-friendly’ layout, and uses some of the same advice given in other guide online and in this project.

Authority:

The guide was written by Ludovic Rembert for Privacy Canada. This is an organisation that is as stated on their homepage a “community run organisation helping Canadians understand cybersecurity”, and their “Canadians right to be forgotten”. (Canada, n.d.)

Purpose:

As stated above the purpose of this source is to provide an online guide to Canadians on their online privacy. The guide is laid out well, uses good, relevant information, and isn’t filled with opinionated jargon that may confuse some readers. The guide is accessible to every type of reader, and has met it’s intended purpose well.

After reading all of these sources, It can be concluded that to create a good, user friendly guide, it would be best to create a guide that provides the reader with enough information to inform them of the privacy risks faced today. And to also write it so that it is simple and not bloated with jargon, so that it can be read fairly quickly, keep interest, and be acted upon. A website that covers steps to protecting users online privacy, with some being more simple, and others more advanced , is a good way to produce a guide based on the research done.

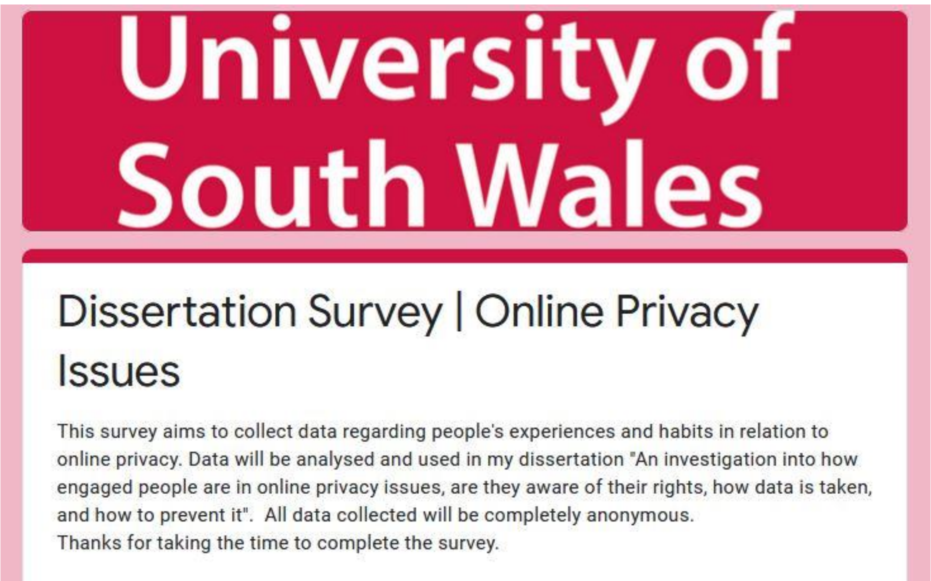
Chapter 3 – Research Methodology:

To look into public opinions on online privacy a simple online survey was created. This anonymous survey, created using Google forms includes basic questions that ask the relevant things while maintaining nuance. The questions asked on the survey were as follow:

- How old are you? (age range of 18-60+)

- Do you consider yourself well-informed on the topic of online privacy, and the rights you have online?
- Do you trust large companies to take care of any data they may have on you?
- Do you think online privacy is more important than getting targeted ads, making websites easier to use etc.?
- Should online privacy be discussed more by the media?
- Have you ever been effected by a data leak?
- If you or someone you know has been effected by a data leak or hacking, how/was the situation resolved?

These questions are mainly focused on the readers' knowledge on the subject, their opinion on these topics, and what can be done to improve things. None of the questions asked are inappropriate, unprofessional, invasive, or un-ethical, and all answers have been recorded anonymously, so there are no legal issues that need to be stated here.



University of South Wales

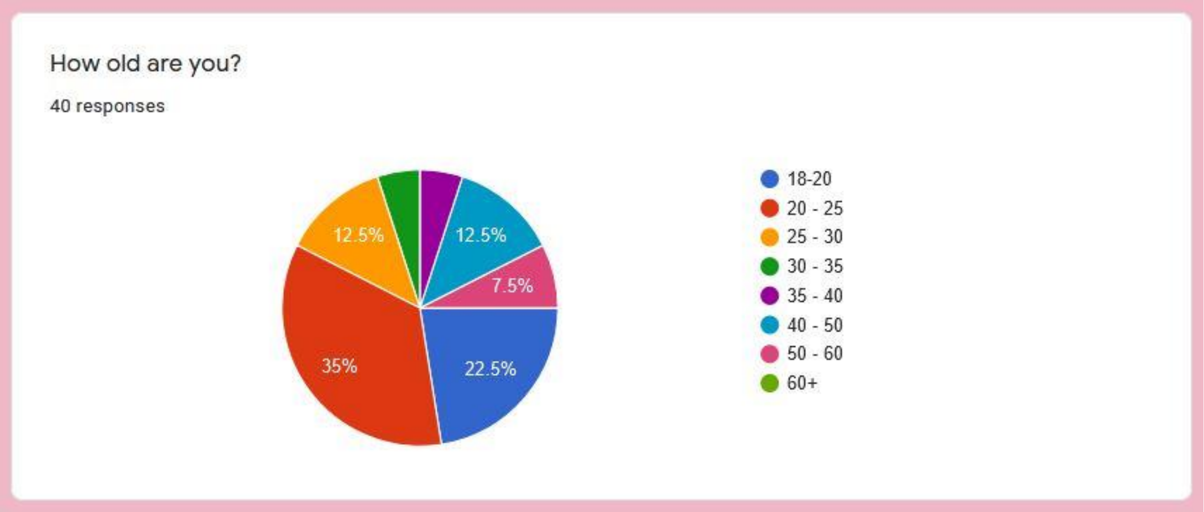
Dissertation Survey | Online Privacy Issues

This survey aims to collect data regarding people's experiences and habits in relation to online privacy. Data will be analysed and used in my dissertation "An investigation into how engaged people are in online privacy issues, are they aware of their rights, how data is taken, and how to prevent it". All data collected will be completely anonymous.
Thanks for taking the time to complete the survey.

Figure 1 - Survey introduction

The start of the survey features a small introduction section that covers what the survey is and any legal issues such as all survey answers being collected anonymously.

The first question the survey asks is how old the user is. As you can see from the chart in figure 2, the survey received a wide range of answers from the 40 different responders. For a wide range of opinions it is vital to have responses from a wide range of ages as the digital literacy level is expected to differ greatly between them. As one would expect, the survey received more responses from those in the younger age ranges. However, as shown the survey did receive responses from older age ranges too. A larger range of younger participants would be expected as they spend more time online, and are therefore more likely to see and respond to the survey.

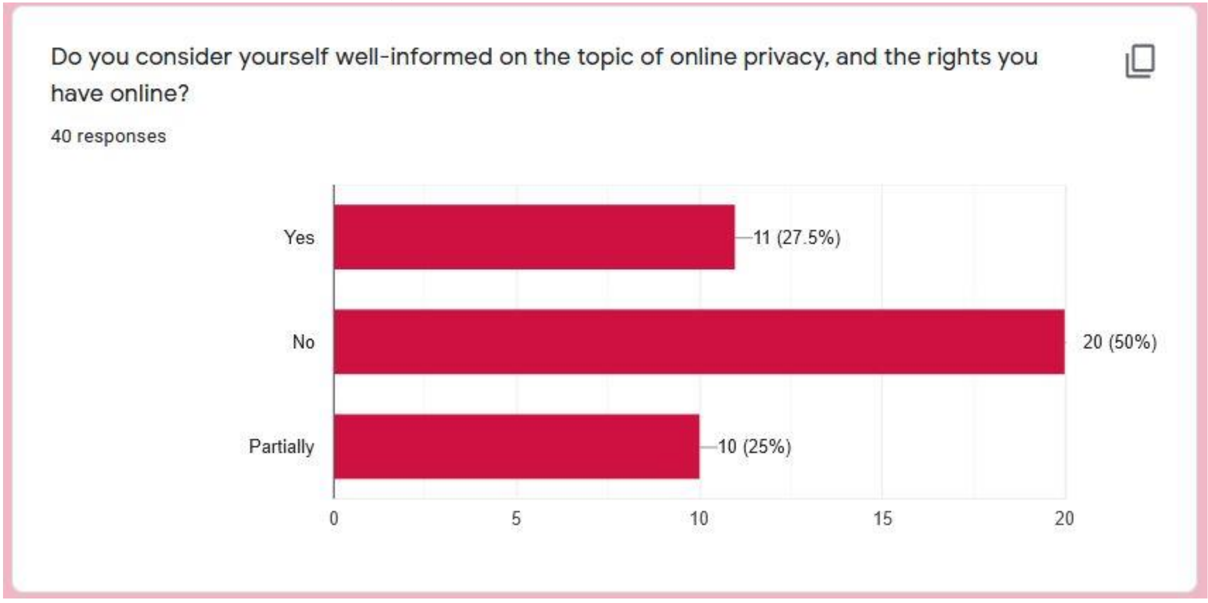


How old are you?

40 responses

Figure 2 - Survey question one

The second question of the survey asks the participant their opinion on their knowledge of online privacy. As shown in figure three below, 50% of participants answered “no” to the question, and 27% answered “yes”, while 25% answered “partially”. These responses provide evidence that most people do not feel well informed about their own online rights and the privacy issues they have online. However when looking at the number of people who responded yes, or partially, we can see that there are a number of people who feel that they have some form of knowledge on these issues. Looking at these results from the responses received, it is surprising that there was not a larger gap between those who feel informed on some level, and those who do not.



Do you consider yourself well-informed on the topic of online privacy, and the rights you have online?

40 responses

Figure 3 - Survey question two

The third question in the survey asks readers do they trust large companies to handle their data. As you can see in figure 4 below, the vast majority of responders (72.5%) answered no. This proves that while most people that responded to the survey do not consider themselves well informed on their online privacy rights, they still overwhelmingly do not trust large companies to hold data they may have of them.

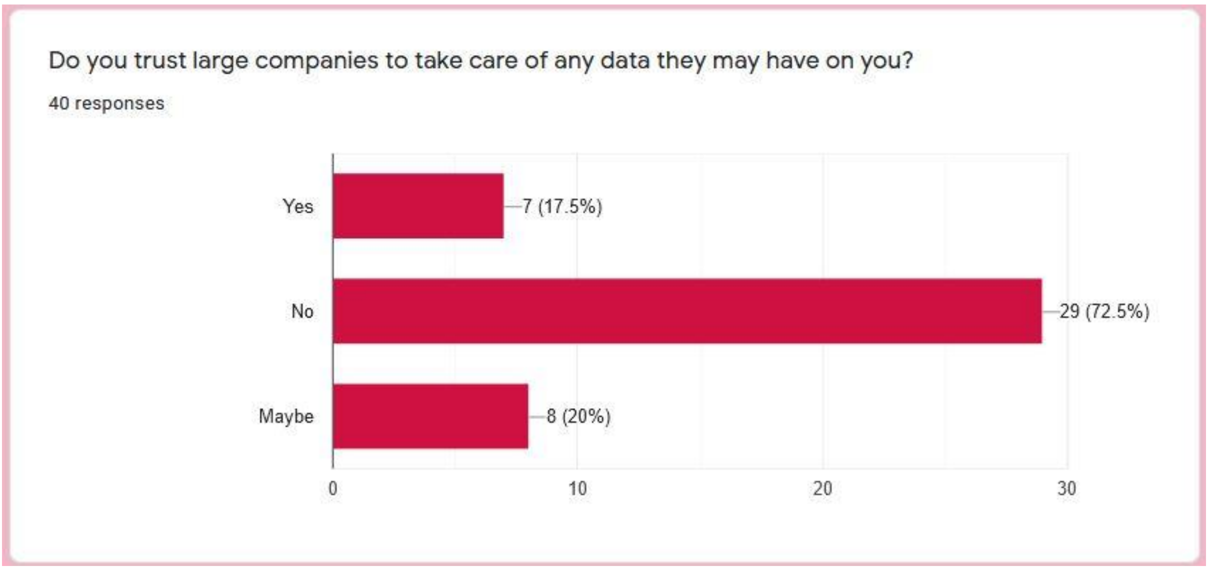


Figure 4 - Survey question three

The fourth question in the survey asks readers if they think online privacy is more important than better site functionality, or receiving targeted advertisements. 72.5% responded yes, 25% answering maybe, and just 5% responded no. Looking at these results, with each question we start to see more clearly that the public do not trust companies to hold their data, and they would like to be more informed on the matter.

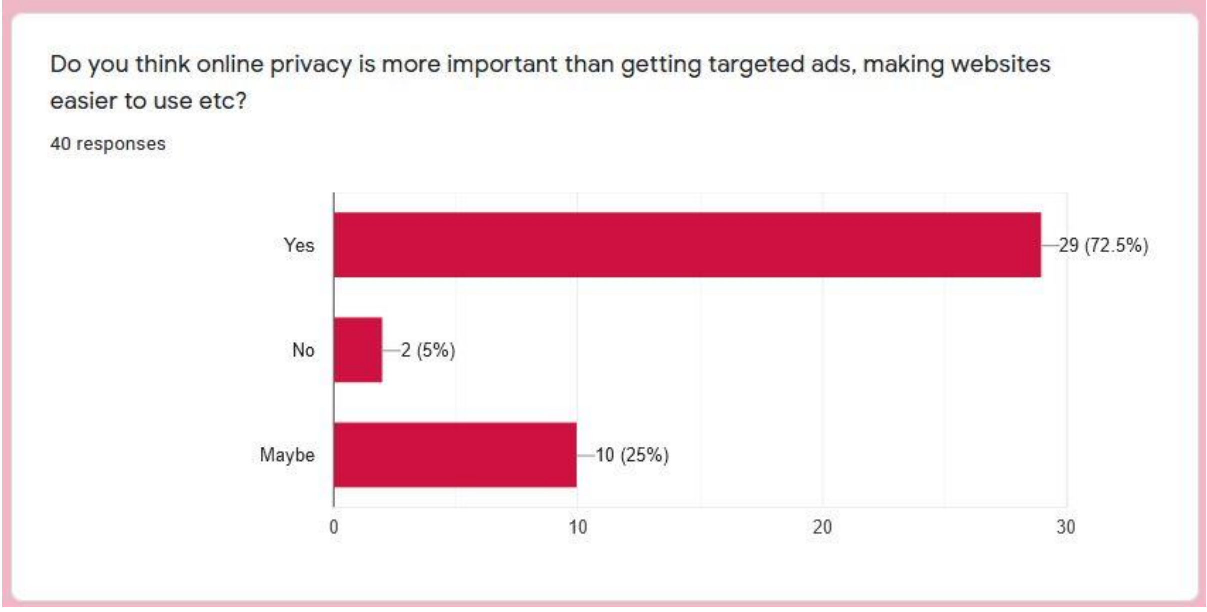


Figure 5 - Survey question four

The fifth question asked in the survey was whether online privacy issues should be discussed more by the media. Based on research shown previously, and the questions asked in the survey so far, it is necessary to ask if people think the issue should be covered more by the media. The research conducted prior to this report shows that when informed on these issues, people tend to change their mind once they have read information presented to them. Figure 6, shown below states that out of those that responded to my survey, 97.5% of people answered yes to the question. This response backs up the previous statement about media coverage, and correlates the initial research done prior to this report. There is clearly a thirst for knowledge on this topic that is becoming more and more engrained into modern life.

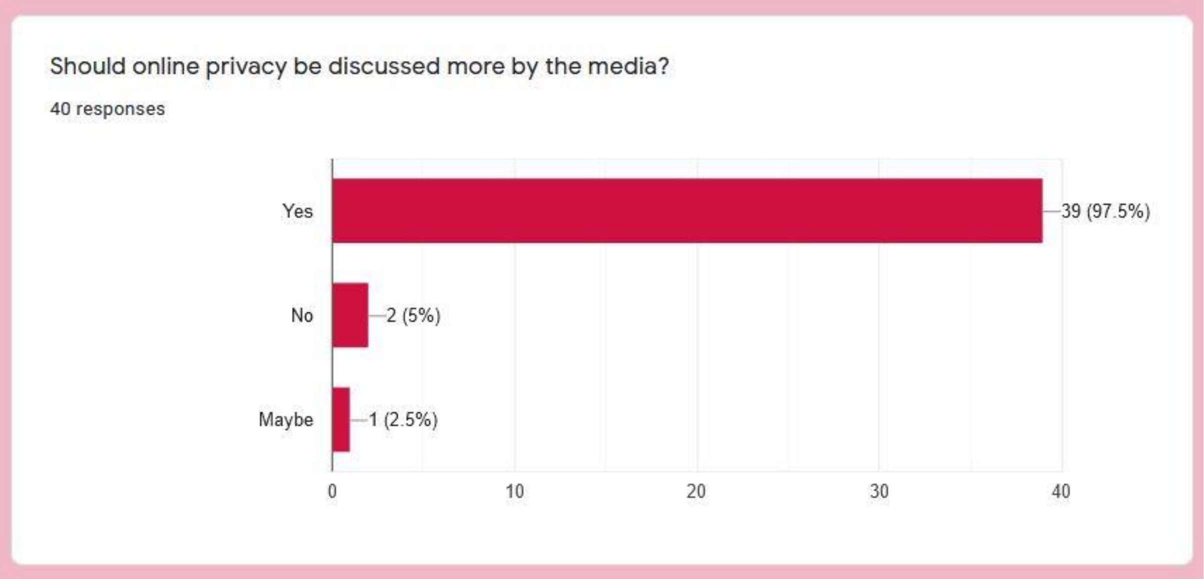


Figure 6 - Survey question five

The sixth question in the survey asks readers if they or someone they know has ever been effected by a data leak or hacking. As you can see in figure 7 below, there was a mix of responses. However, the majority of responses were yes in one form or another. 40% of people responded with “someone I know”, and 27.5% of people responding yes. When creating the survey I added the comment functionality that allowed responders to write a response. As you can see in figure 7 below, most people that responded yes went on to explain that their passwords or banking information had been stolen. These responses again correlate with the research done prior to the report and is expected. “Account takeovers (when thieves gain access to accounts and change passwords) are the fastest growing sector of identity theft, with a massive 61% increase.” *(Henshaw, Sandra, Tiger Mobiles, 2019)*

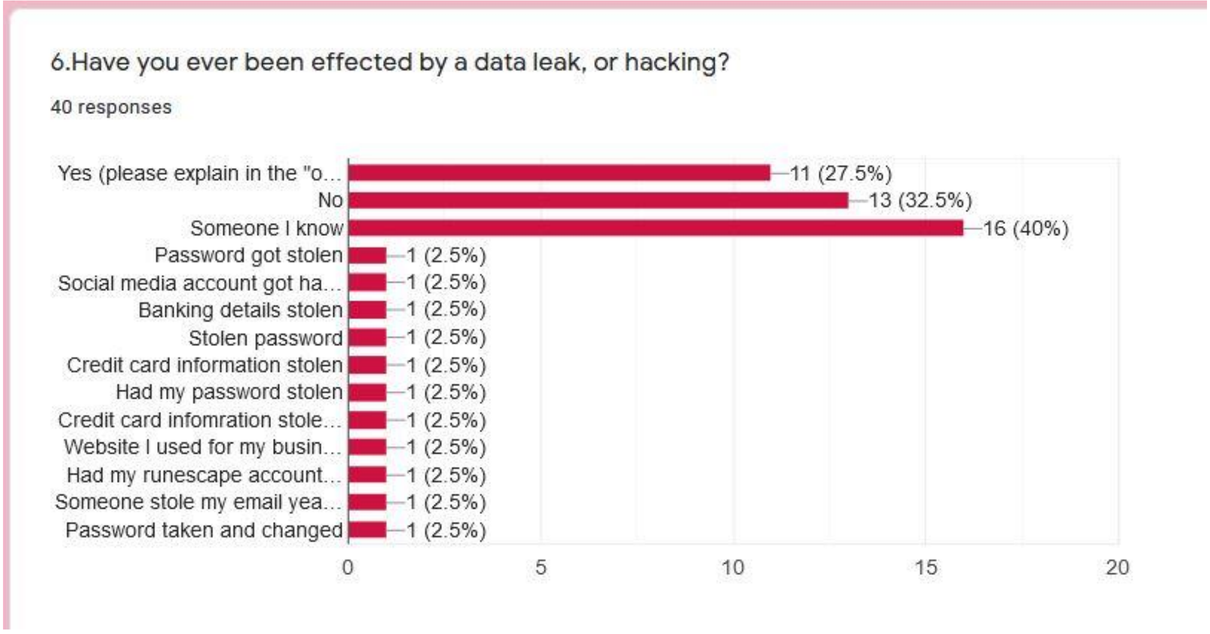


Figure 7 - Survey question six

The seventh and final question in the survey relates to the previous question and asks if users were affected by a data leak, how or was the situation resolved. Looking at figure eight below, we can see that 56.7% responded with “organisational involvement (data leak). The results show that the majority of incidents were resolved without police involvement, with many incidents being resolved personally, or through an organisation. The results to this question was expected as with most cases of data leak and the results shown in figure six, the majority of these were stolen passwords or banking information. As these can be used for serious crimes such as identity theft, and fraud, in the most serious instances some form of organisational or police involvement is necessary.

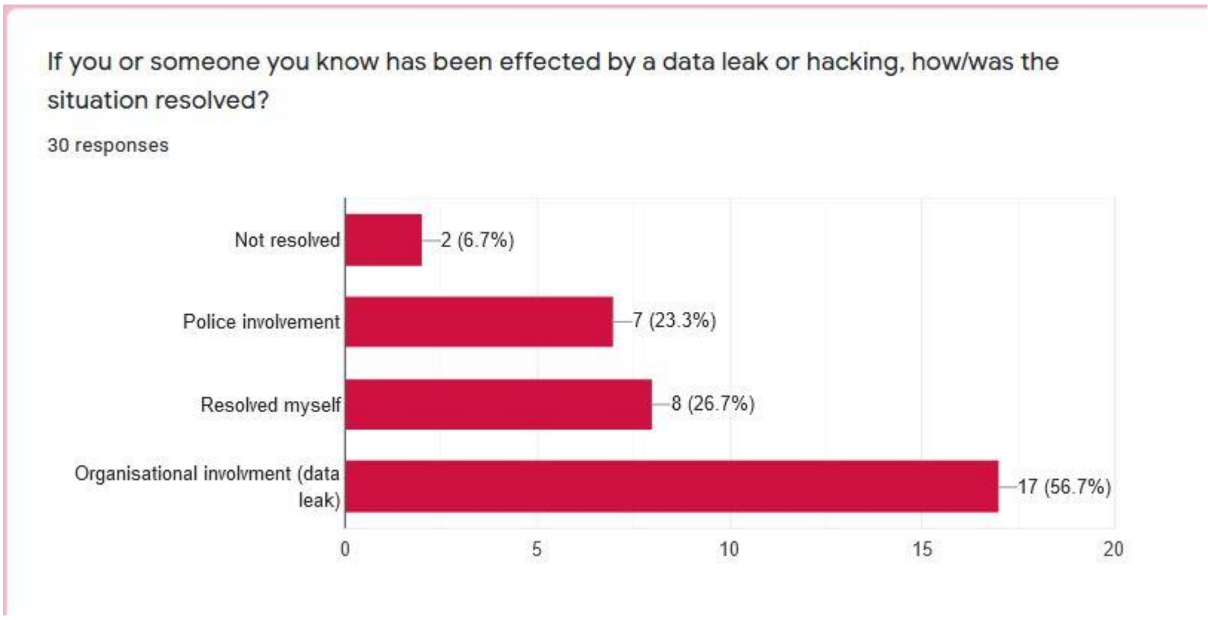


Figure 8 - Survey question seven

Chapter 4 – Design and Development:

The guide to online privacy is a website that offers an accessible guide to protecting your privacy while using the web. The site offers a simple guide that is delivered as a ‘package’ that covers the common ways that people obtain information. It covers text based, and image based methods of conveying information. The website was designed on paper to be very simple, easy to use, and quick on load times so that the guide can be read no matter the users’ situation. This could be having a slow PC, unstable internet connection, or on a smartphone. The website is very fast to load as it uses just HTML, CSS, JavaScript, and makes no use of backend development such as php, and does not call any information from a database like a lot of websites in use today. The site also features no tracking cookies of any kind; this can greatly reduce load times.

4.1 – Initial Designs:

The site was designed firstly via pen and paper methods. Once a layout had been decided upon, a mock-up was created before production began. The designs can be seen below.

Home Page:

As seen in figure 9 to the left, this mock-up shows the basic outline for the home page, and what content will be found on it.

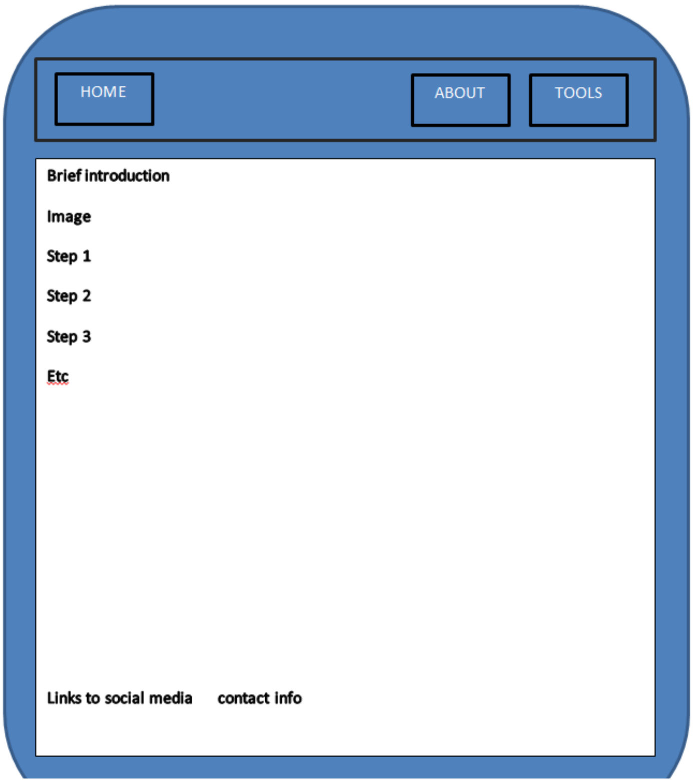
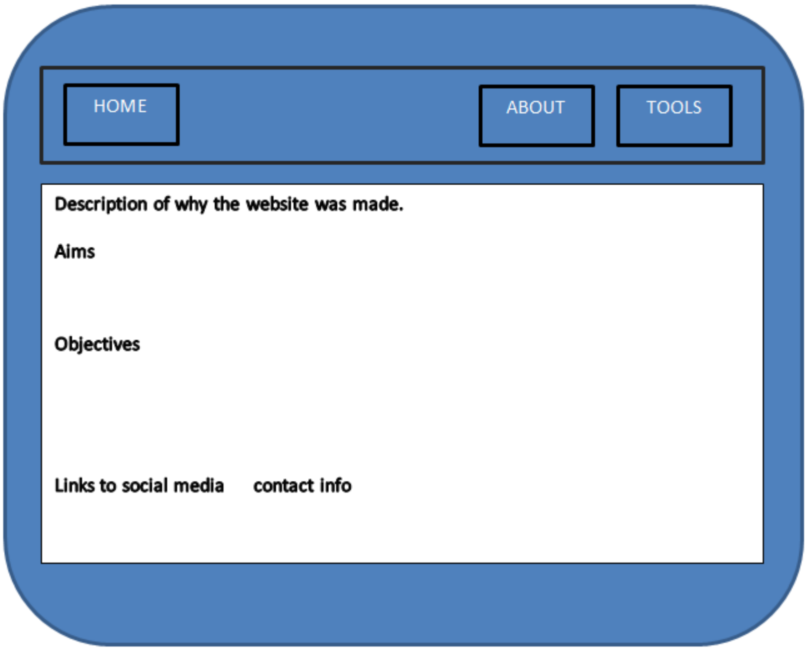


Figure 9 – Home Page mock-up

About Page:



Description of why the website was made.

Aims

Objectives

Links to social media contact info

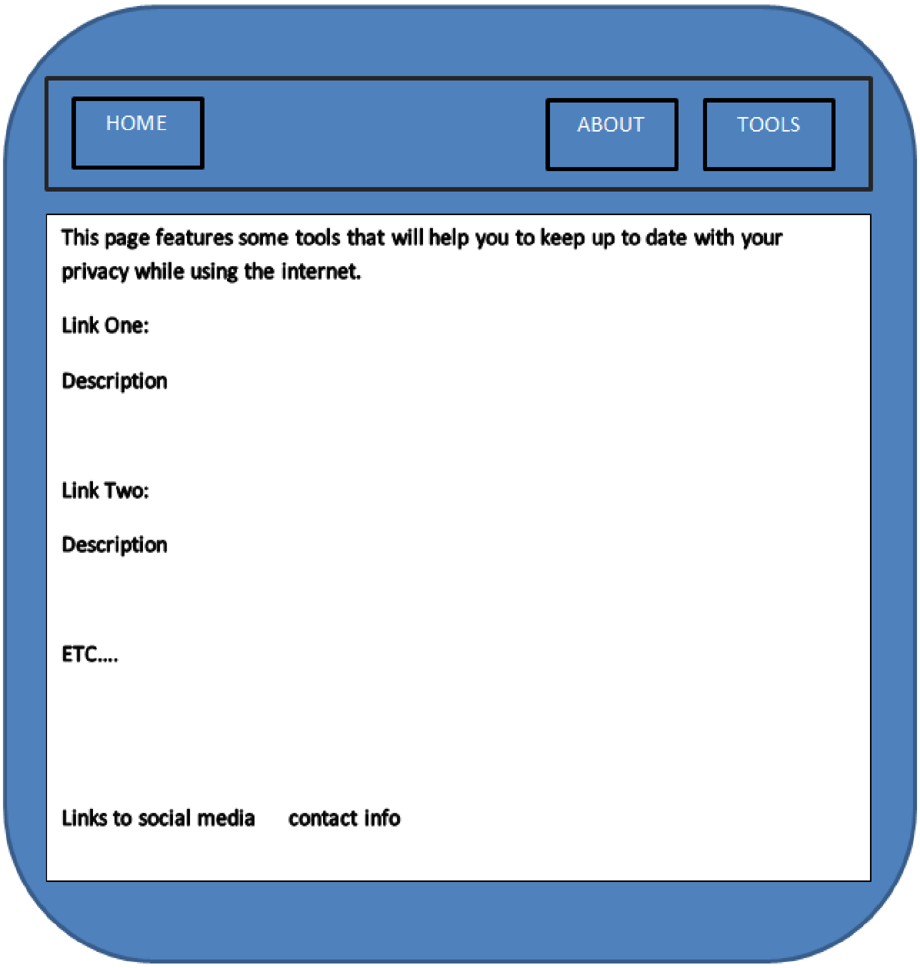
Figure 10 - About Page mock-up

Figure 10 show that the about page features the same basic layout design used in the home page. However, it features different content.

The minimalist design is kept the same to remain consistent and easy to use.

Tools Page:

Figure 11 show the final page. The tools page is again using the same design layout, for the reasons listed above. This page's purpose is to provide the reader with useful links/tools. And give a brief explanation.



This page features some tools that will help you to keep up to date with your privacy while using the internet.

Link One:

Description

Link Two:

Description

ETC....

Links to social media contact info

Figure 11 - Tool Page - Mock-up

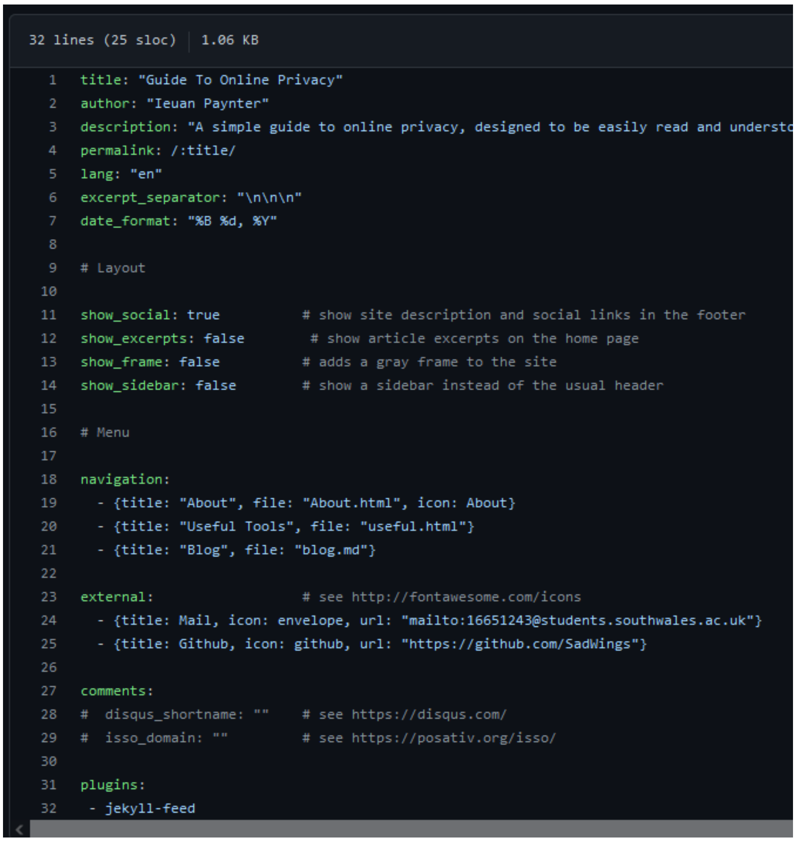
4.2 – Production:

This website was created using Jekyll and GitHub. Jekyll is a static site generator that creates websites from templates. These templates can be created using a wide variety of languages, such as html, CSS, python, JavaScript, and most commonly markdown. Templates can be easily downloaded and edited using GitHub. GitHub is a git hosting service that allows users to collaborate and share projects online. A git is an open source version control system, this means that developers can continually make changes to programmes and release new versions. GitHub is a place where developers can store, share, and release software in this method.

This website was created using a simple theme found on Jekyll's theme section, forked on GitHub, and then edited using the markdown language. The theme used is free for use, and open source. This means that the website can be built with this theme as its design inspiration, edited to fit the websites needs, and be 'lightweight' meaning is it fast, responsive, and easily loadable for readers.

Figure 12 below, shows the configuration file of the website on GitHub, used to edit the site.

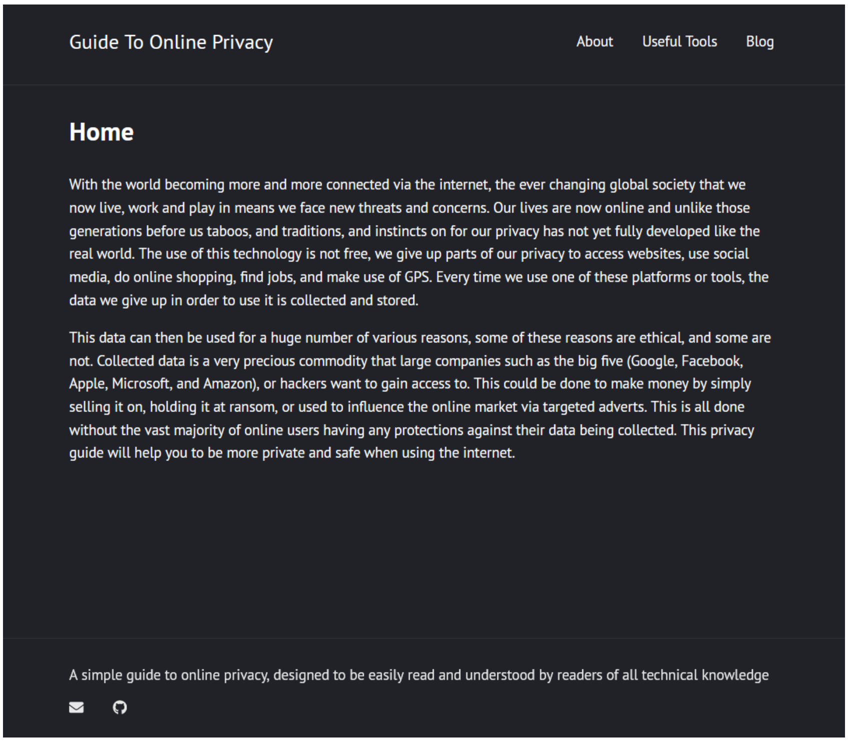
This configuration file also shows markdown language being used and implemented. Figure 12 shows just how simple the language is to use; for example at the start of the document, the title, author and description are all easily understood.



```
32 lines (25 sloc) | 1.06 KB

title: "Guide To Online Privacy"
author: "Ieuan Paynter"
description: "A simple guide to online privacy, designed to be easily read and understo
permalink: /:title/
lang: "en"
excerpt_separator: "\n\n\n"
date_format: "%B %d, %Y"

# Layout

show_social: true          # show site description and social links in the footer
show_excerpts: false        # show article excerpts on the home page
show_frame: false          # adds a gray frame to the site
show_sidebar: false        # show a sidebar instead of the usual header

# Menu

navigation:
  - {title: "About", file: "About.html", icon: About}
  - {title: "Useful Tools", file: "useful.html"}
  - {title: "Blog", file: "blog.md"}

external:                  # see http://fontawesome.com/icons
  - {title: Mail, icon: envelope, url: "mailto:16651243@students.southwales.ac.uk"}
  - {title: Github, icon: github, url: "https://github.com/SadWings"}

comments:
#  disqus_shortname: ""    # see https://disqus.com/
#  isso_domain: ""         # see https://posativ.org/isso/

plugins:
 - jekyll-feed
```

Figure 12 - Website Configuration file

The following image showcases these designs in production before the main content is added.



Home

With the world becoming more and more connected via the internet, the ever changing global society that we now live, work and play in means we face new threats and concerns. Our lives are now online and unlike those generations before us taboos, and traditions, and instincts on for our privacy has not yet fully developed like the real world. The use of this technology is not free, we give up parts of our privacy to access websites, use social media, do online shopping, find jobs, and make use of GPS. Every time we use one of these platforms or tools, the data we give up in order to use it is collected and stored.

This data can then be used for a huge number of various reasons, some of these reasons are ethical, and some are not. Collected data is a very precious commodity that large companies such as the big five (Google, Facebook, Apple, Microsoft, and Amazon), or hackers want to gain access to. This could be done to make money by simply selling it on, holding it at ransom, or used to influence the online market via targeted adverts. This is all done without the vast majority of online users having any protections against their data being collected. This privacy guide will help you to be more private and safe when using the internet.

A simple guide to online privacy, designed to be easily read and understood by readers of all technical knowledge

Figure 13 - Home Page Final Design

As figure 13 shows, the design is very minimalistic, and conveys the content well as it is left to stand out and focus the reader’s attention. The Navigation bar at the top of the screen is easy to use and not distracting. At the bottom of the page links to contact via email, and a link to the GitHub page can be seen.

Chapter 5 – The Connected World:

Today’s world is an ever changing one, since the 90’s society has grown more and more accustomed to the internet, an interconnected web of seemingly endless information that connects us all together. With this societal embrace of the internet we have gained new ways to work, learn, socialise, and shop from anywhere with an internet connection. While this interconnected world we live in has brought many benefits, it also has many negatives. So much of our lives are now online that we leave “digital footprints” of nearly every aspect of our lives; these “footprints” are used to build up an “image” of our hobbies, interests, our online purchases, the people we share our interests with and even in some cases, where we work, live and frequently visit. This may sound confusing, but the way large companies such as Amazon or YouTube know what to suggest you, is by using these digital footprints to build up an image of your habits. This built up collection of data, once collected and sent off to the relevant places is then used for targeted advertisements, or sold off to data collectors and used for even more reasons. People have very differing opinions on data collection and our online privacy; some people view it as a “trade-off” where we give up some of our privacy and allow data to be collected, so that we receive personal, targeted ads, can share data between online platforms easier, and view some websites that require cookies, or view our location to give directions. Other people view this trade-off as a negative thing. They generally see it as; yes giving up our information may make navigating the web and our online lives more simple. However, giving out information about our personal lives is not. As stated above this collected information is used for many different things, and I will now explain how this data is collected.

Chapter 6 – Online Privacy Laws:

In the UK the main set of laws that cover data is the infamous data protection act of 2018 or more commonly known as GDPR, or the general data protection regulations. The regulations, first set up in 2016 under EU law covered the laws on data collection, privacy and security. It is still considered the strictest set of privacy regulations in the world. The laws were put into place in 2018 across EU member states to set up a standard of consumer privacy for all organisations and business that collect or handle data of EU citizens. Failing to comply with GDPR could mean facing heavy fines; there are slight differences in some regions however. Violating GDPR will mean a fine of 4% of global revenue from the previous financial year. With the UK leaving the EU this year after Brexit, there have been slight changes to the laws in the UK. The EU's GDPR no longer applies to the UK, however as the GDPR was implemented into UK law in 2018, not much will change. The UK government, now that we have left the EU, will be able to make changes to GDPR. For the ease of understanding, the UK's version is labelled; UK GDPR, and the EU's, GDPR. Both UK and EU citizens will be covered by GDPR under the Brexit agreements; however data leaving the UK and into the EU will be covered by the EU GDPR, where as if it stays within the UK, then it is covered by UK GDPR.

The GDPR covers seven principles designed to maintain data protection, security, and accountability. These seven principles are as follow;

- Lawfulness, fairness, and transparency:

All data collected and stored, as well as the reasoning behind the collection must be made transparent to the public and made available upon request.

- Purpose limitation:

All personal data collected must be done so for legitimate reasons, and made available to the public. This is to ensure that data is taken and used only for the reasons stated.

- Data minimisation:

All collected data must be relevant and limited to the stated and necessary reasons it was collected. This is done to endure that only the relevant data is collected and stored, not all the personal data an organisation could collect.

- Accuracy:

All personal data collected, must be kept up to date and accurate.

- Storage limitation:

Organisations must only hold personal data for the necessary time needed and for the purpose it was collected for. Once it has been used, it must be deleted or "cleansed".

- Integrity and confidentiality:

All data must be stored in the appropriate and secure way. The correct levels of security must be in place to deal with all types of data and all data must be encrypted.

- Accountability:

When dealing with data, organisations must take accountability for the data and comply with GDPR. Evidence of compliance must be recorded, and current practises should be reviewed regularly.

(Information commisioners office, 2018)

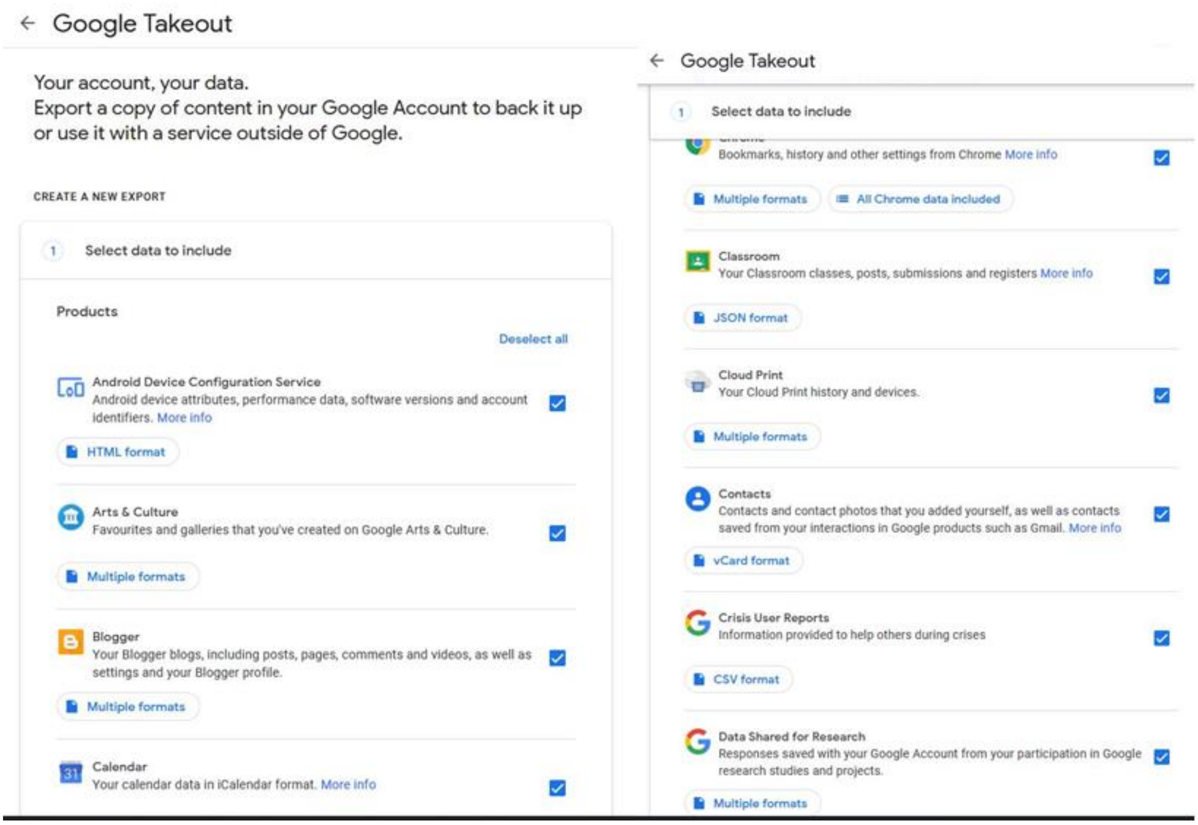
Any data from the UK that goes abroad to places such as the US, Canada, Australia, Japan, etc. must comply with UK GDPR. This means that large platforms such as Google, Facebook, Apple, Microsoft, and Amazon (known as the big five) will have to make changes to the way they handle data from the UK compared to data coming from elsewhere with less strict privacy laws. GDPR changes the way companies collect and handle personal data, while this does mean companies are unable or less likely to breach privacy laws, they are also able to continue collecting personal data, as long as the user agrees to it, and the data is handled correctly in-line with local laws such as GDPR. Back in 2018 when GDPR was initialized you may remember every site you visited having some form of pop up message in regards to "changes to our privacy policy" this was due to GDPR and the changes it made to our online privacy. GDPR has given the internet user much more control and transparency over our personal data online. Before the regulations came into place companies such as the big five listed earlier where free to collect and sell our data with very little agreement from their users. Now if an organisation needs to collect and store your personal data, they will have to inform you why, and handle the data transparently. While GDPR means much more transparency and control over our own personal data, there are loopholes for large companies and at the time of implementation, high costs for training and preparedness for smaller companies afraid of breaching the new rules and regulations. While the GDPR face some criticism when it was announced, the vast majority of reaction was positive. Scandals such as the Cambridge analytica scandal has led to more and more open support of online privacy and laws such as GDPR.

Chapter 7 – How Is data collected?

The internet isn't free, once you've paid the bills to gain access to the internet you then have to give up certain levels of personal data to access websites or use certain programs. This could simply be creating an account where an email or even first and last names are required, accepting targeted ads, or browser cookies. All of these require some form of privacy to be given up, and more importantly, all of these are linked to methods used for data collection. Another hugely important method is simply asking for it, when using most sites today you will be greeted with a privacy, or cookie policy. These pop-ups will cover the organisations policies on browser cookies, pixel tags, copyright rights, and the use of this data. These methods of data collection work in many different ways, some more specific than others. For example; the methods listed allow organisations to track browser history of the user, even after they have left the site. This data is then logged and used for targeted ads, and in some instances, possibly sold on to other organisations.

7.1 – Personal Data Collected:

Simply searching "download my Google data" will take you to a Google page that allows you to download and view the data Google has on you. Before even selecting the download method, you are greeted with a page that shows the potential places Google has available data stored on you. You may be surprised to see how much data is available.



Google Takeout

Your account, your data.
Export a copy of content in your Google Account to back it up or use it with a service outside of Google.

CREATE A NEW EXPORT

1 Select data to include

Products

Deselect all

Android Device Configuration Service
Android device attributes, performance data, software versions and account identifiers. More info ☑
HTML format

Arts & Culture
Favourites and galleries that you've created on Google Arts & Culture. ☑
Multiple formats

Blogger
Your Blogger blogs, including posts, pages, comments and videos, as well as settings and your Blogger profile. ☑
Multiple formats

Calendar
Your calendar data in iCalendar format. More info ☑

Google Takeout

1 Select data to include

Bookmarks, history and other settings from Chrome More info ☑
Multiple formats | All Chrome data included

Classroom
Your Classroom classes, posts, submissions and registers More info ☑
JSON format

Cloud Print
Your Cloud Print history and devices. ☑
Multiple formats

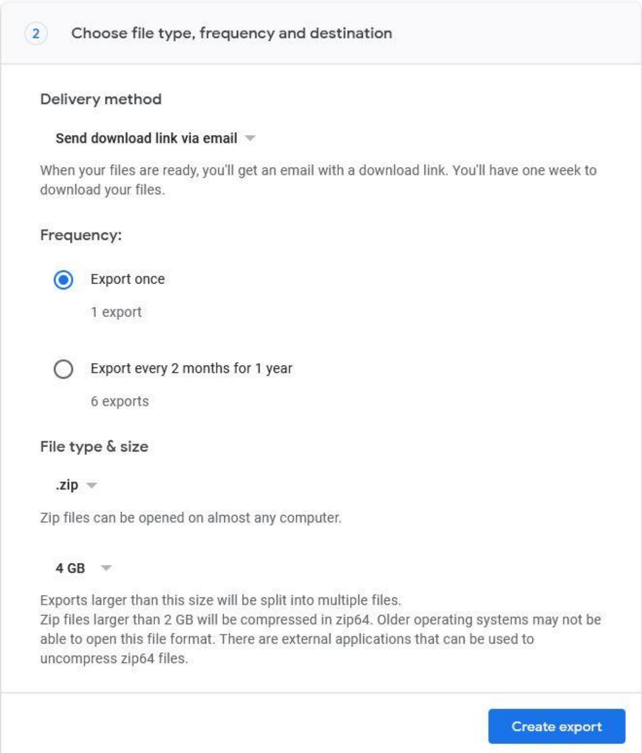
Contacts
Contacts and contact photos that you added yourself, as well as contacts saved from your interactions in Google products such as Gmail. More info ☑
vCard format

Crisis User Reports
Information provided to help others during crises ☑
CSV format

Data Shared for Research
Responses saved with your Google Account from your participation in Google research studies and projects. ☑
Multiple formats

Figure 14 - Possible Google data

As figure 14 shows above, the amount of data Google could possibly have on you can ne shocking if not monitored correctly. When going through the steps to download your data, you can also select a frequency of when your data is downloaded and the export method, file type, and file size. This is shown in figure 15 below.



2 Choose file type, frequency and destination

Delivery method

Send download link via email

When your files are ready, you'll get an email with a download link. You'll have one week to download your files.

Frequency:

● Export once

1 export

○ Export every 2 months for 1 year

6 exports

File type & size

.zip

Zip files can be opened on almost any computer.

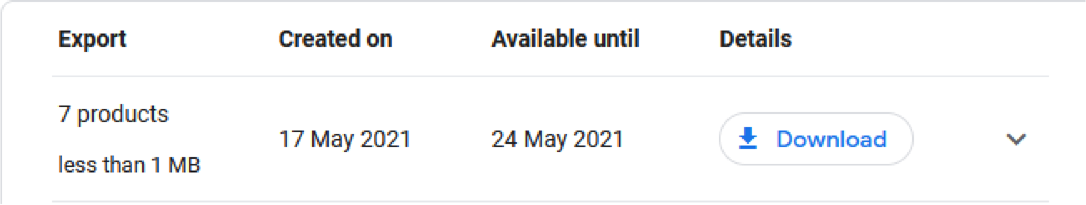
4 GB

Exports larger than this size will be split into multiple files.
Zip files larger than 2 GB will be compressed in zip64. Older operating systems may not be able to open this file format. There are external applications that can be used to uncompress zip64 files.

Figure 15 - Google data export options

Once you have selected these options, you will then be greeted with an estimated time; this could take from a few hours, up to a few days depending on the amount of available data.

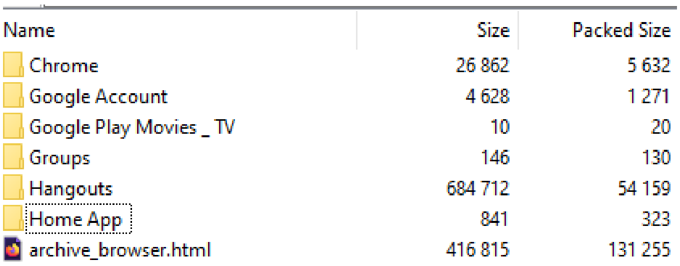
Once this download from Google has been completed, you will receive an email with your download link and your data request, as shown in figure 15 below.



Export	Created on	Available until	Details
7 products less than 1 MB	17 May 2021	24 May 2021	Download

Figure 16 - Download link

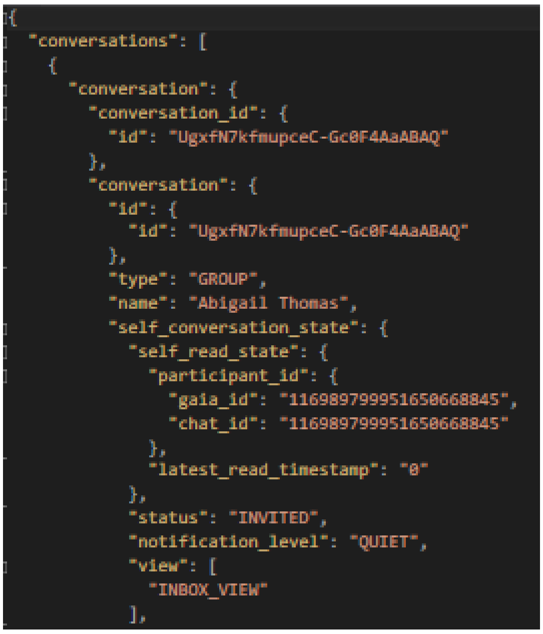
For the purpose of saving time a very short and brief data request from Google was requested, these can be ready to download within five minutes. As you can see from the images below, even though a very small amount of data was downloaded, Google still had a large amount of personal data stored. This stored data covers topics such as account information, search history, any Google play movies watched, Google groups and its members, Google hangouts, and information from the Google home app linked to Google home devices within consumers'homes.



Name	Size	Packed Size
Chrome	26 862	5 632
Google Account	4 628	1 271
Google Play Movies _ TV	10	20
Groups	146	130
Hangouts	684 712	54 159
Home App	841	323
archive_browser.html	416 815	131 255

Figure 17 - Google data

When looking at the raw data in these files, one can see just how much of our data is recorded and kept online. Figure 18 below is the raw data from the Google hangouts chat service; the data shown here is taken from chats in 2016/17.



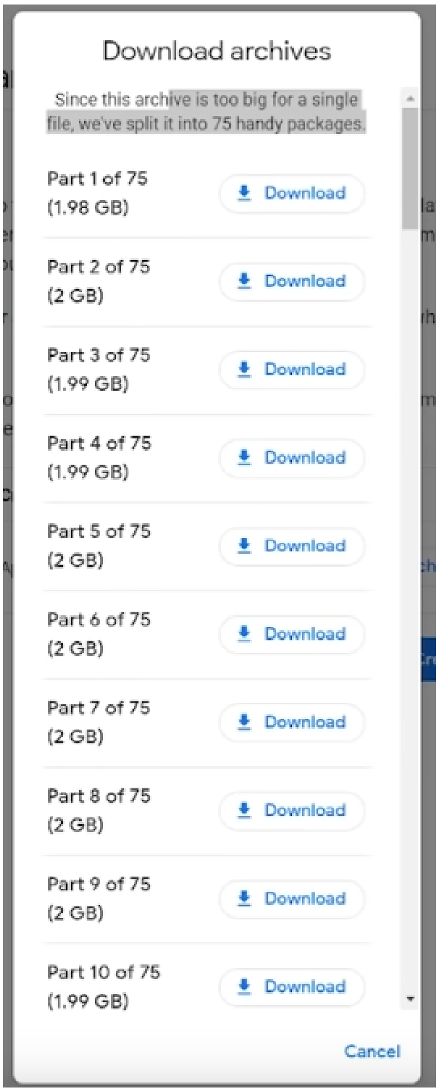
```
{
  "conversations": [
    {
      "conversation": {
        "conversation_id": {
          "id": "UgxfN7kfmupceC-Gc0F4AaABAQ"
        },
        "conversation": {
          "id": {
            "id": "UgxfN7kfmupceC-Gc0F4AaABAQ"
          },
          "type": "GROUP",
          "name": "Abigail Thomas",
          "self_conversation_state": {
            "self_read_state": {
              "participant_id": {
                "gaia_id": "116989799951650668845",
                "chat_id": "116989799951650668845"
              },
              "latest_read_timestamp": "0"
            },
            "status": "INVITED",
            "notification_level": "QUIET",
            "view": [
              "INBOX_VIEW"
            ],
```

As you can see, the data contains things such as conversation id's, message types, the group notification level, and even names.

Figure 18 - Google hangouts data

When this feature was first made available to Google users a few years ago (due to laws and regulations such as GDPR) many people would wait months for their data to arrive, and the results caused mass distrust, and outrage towards Google. More privacy is now demanded and required by law.

Figure 18, shows just how much of his personal data Devon Crawford was able to download from Google. *(Downloading My Private Google Data, this is what I found, 2019)*



Download archives

Since this archive is too big for a single file, we've split it into 75 handy packages.

Part 1 of 75 (1.98 GB) Download

Part 2 of 75 (2 GB) Download

Part 3 of 75 (1.99 GB) Download

Part 4 of 75 (1.99 GB) Download

Part 5 of 75 (2 GB) Download

Part 6 of 75 (2 GB) Download

Part 7 of 75 (2 GB) Download

Part 8 of 75 (2 GB) Download

Part 9 of 75 (2 GB) Download

Part 10 of 75 (1.99 GB) Download

Cancel

As you can see the amount of data was so large that it had to be split into 75 different packages to be downloaded at the 2GB cap Devon had set. Google has recently changed its privacy policy to allow users to edit what permissions Google have on what data can be taken. They have also recently stated that they will start deleting data for new users after a set time. *(Alexander Maxham - Android Headlines, 2020)*

Figure 19 (left) large data download

Another infamous case of data collection is the Facebook/ Cambridge Analytica scandal. Cambridge analytica was a political consulting firm based in London that supported political campaigns in both the UK and the US using data science. The firm gathered data from social media accounts on platforms such as Facebook, to build up profiles of up to 90 million users so that their political views could be influenced. *(Jason Fernando - Investopedia, 2021)* Once a "profile" of a person had been built up using data found on their account from the pages they like, posts they share, and the friends they interact with, specific ads, websites, personality quizzes, or even apps would be created and shown to users so that their views could be altered until there were visible changes. When a user clicks on some of the things listed here, such as a personality quiz, they would be informed that in order to use this app or complete this quiz they would be agreeing to give access to all their personal data on their accounts, and also their friends list. This is how Cambridge analytica was able to gain the information of so many users within a few short months. All of this was also completely legal under UK law at the time.

These algorithms, built up by harvesting personal data, and used to modify behaviour were finally revealed to the public in 2018 by whistle blower Christopher Wylie. In 2018 he met with journalists from the Guardian and gave evidence of the firm's doings using people's personal data from Facebook. Once the documents had been put together and released to the public by the Guardian, governments commenced mass, thorough investigations into Cambridge analytica and their data scraping exercise. These investigations, along with evidence given by whistle-blowers such as Christopher Wylie, or Brittany Kaiser, led to the firm facing multiple international lawsuits that saw Cambridge analytica declare bankruptcy in 2018. After this many social media users became much more aware of exactly what they were sharing online, looked at privacy policies more, and some even deleted there accounts. The #deleteFacebook trend began and Facebook saw a massive decline in its users as trust in the platform had been broken.

7.2 – How Can Data Collection Be Stopped/ Controlled:

There are a number of many different ways of preventing your personal data being collected. Some are more successful, some more complicated and less complicated than others, but these methods will reduce the amount of personal data that can be collected online. Firstly, it should be stated that the only way to truly stop all of your personal data being collected online is to stop using the internet. As said in my introduction, today's world is and interconnected hive of ever-changing information. To be a part of that online world and make use of things such as social media, email, or simply internet browsing is to accept that some of your personal data will be collected. The only way to stop all personal data being collected is to remove oneself from the online world. This however does not need to be done to be safe, and secure while online. To prevent data collection, some sacrifices will need to be made depending on your desired level of privacy.

Chapter 8 – Implementation (Guide to online privacy):

With the world becoming more and more connected via the internet, the ever changing global society that we now live, work and play in means we face new threats and concerns. Our lives are now online and unlike those generations before us taboos, and traditions, and instincts on for our privacy has not yet fully developed like the real world. The use of this technology is not free, we give up parts of our privacy to access websites, use social media, do online shopping, find jobs, and make use of GPS. Every time we use one of these platforms or tools, the data we give up in order to use it is collected and stored. This data can then be used for a huge number of various reasons, some of these reasons are ethical, and some are not. Collected data is a very precious commodity that large companies such as the big five (Google, Facebook, Apple, Microsoft, and Amazon), or hackers want to gain access to. This could be done to make money by simply selling it on, holding it at ransom, or used to influence the online market via targeted adverts. This is all done without the vast majority of online users having any protections against their data being collected. This privacy guide will help users to be more private when using the internet. The guide will cover a few key basic steps one can take, and then some advanced steps for a higher level of privacy.

The guide to online privacy website can be found at: https://sadwings.github.io/

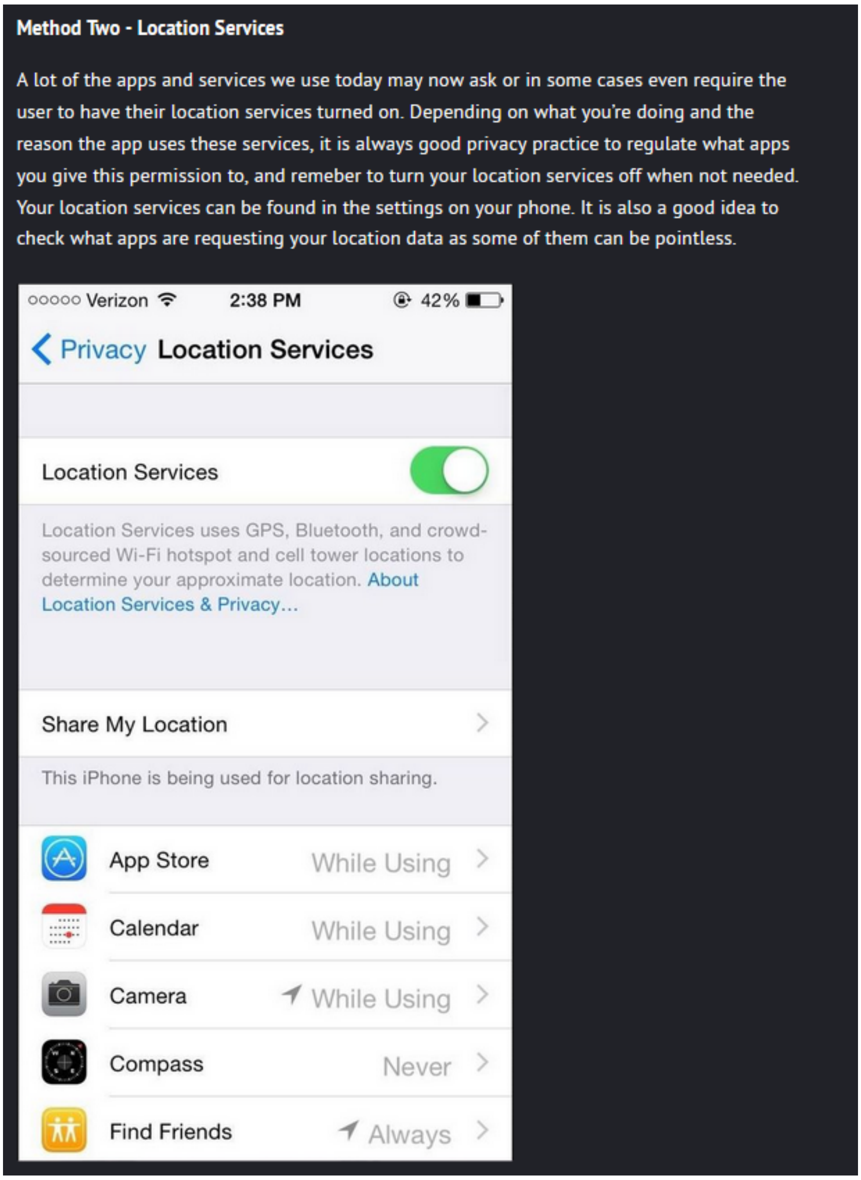
The website is an easily accessible and user-friendly guide to online privacy, designed with a few key points in mind. These points are as follow:

- Ease of navigation – This website must be easy to use and understand by users of all technological knowledge levels.
- Minimalist design choice – To keep the site simple to navigate, and draw focus to the content, a minimalist design aesthetic was chosen. This also makes the site very fast, responsive, and easy to load.
- User friendly – The guide must be easy to read and understandable, the guide provides the reader with different steps they can take to care take their online privacy and is delivered using both text and images. It is important that the reader is not hammered with mass amounts of text, technical jargon, or biased.

The finished version of the website meets the design aims & objectives, and more importantly the aims of delivering easily digestible content.

The website gives readers different steps one can take to increase their online privacy and in some cases cyber security. The advice given provides brief explanations of what the topic is, how it affects the reader, and what can be changed. There are also supporting images that feature alt text for those with sight issues.

Topic example:



Method Two - Location Services

A lot of the apps and services we use today may now ask or in some cases even require the user to have their location services turned on. Depending on what you're doing and the reason the app uses these services, it is always good privacy practice to regulate what apps you give this permission to, and remeber to turn your location services off when not needed. Your location services can be found in the settings on your phone. It is also a good idea to check what apps are requesting your location data as some of them can be pointless.

Location Services ●

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy…

Share My Location

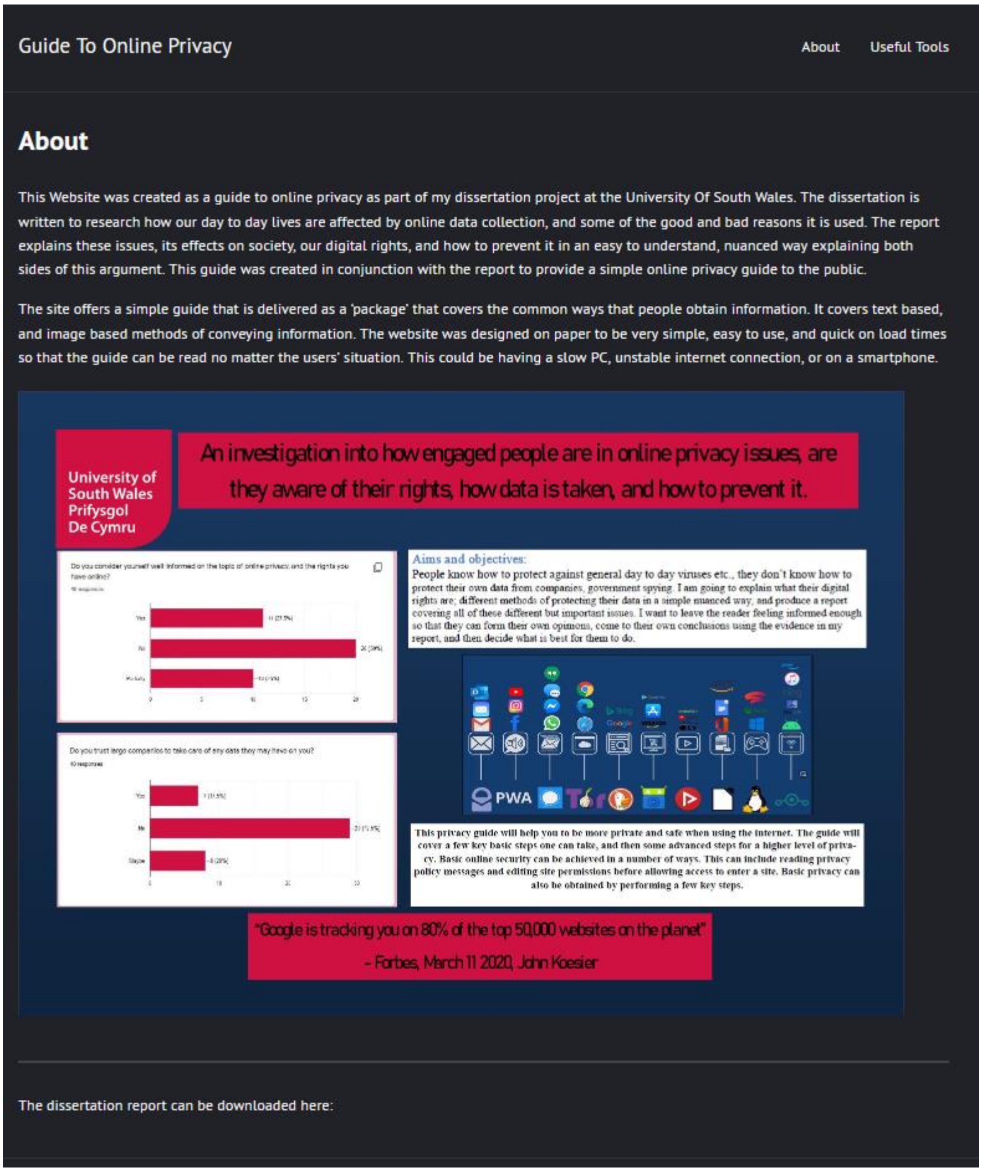
This iPhone is being used for location sharing.

App Store	While Using
Calendar	While Using
Camera	While Using
Compass	Never
Find Friends	Always

Figure 20 - Website topic example

About page:

The about section of the website covers the reason for the site being created, what it offers, a poster for the project and a link to download the project report.



About

This Website was created as a guide to online privacy as part of my dissertation project at the University Of South Wales. The dissertation is written to research how our day to day lives are affected by online data collection, and some of the good and bad reasons it is used. The report explains these issues, its effects on society, our digital rights, and how to prevent it in an easy to understand, nuanced way explaining both sides of this argument. This guide was created in conjunction with the report to provide a simple online privacy guide to the public.

The site offers a simple guide that is delivered as a 'package' that covers the common ways that people obtain information. It covers text based, and image based methods of conveying information. The website was designed on paper to be very simple, easy to use, and quick on load times so that the guide can be read no matter the users' situation. This could be having a slow PC, unstable internet connection, or on a smartphone.

An investigation into how engaged people are in online privacy issues, are they aware of their rights, how data is taken, and how to prevent it.

Do you consider yourself well informed on the topic of online privacy, and the rights you have online?

Do you trust large companies to take care of any data they may have on you?

Aims and objectives:
People know how to protect against general day to day viruses etc., they don't know how to protect their own data from companies, government spying. I am going to explain what their digital rights are; different methods of protecting their data in a simple nuanced way, and produce a report covering all of these different but important issues. I want to leave the reader feeling informed enough so that they can form their own opinions, come to their own conclusions using the evidence in my report, and then decide what is best for them to do.

This privacy guide will help you to be more private and safe when using the internet. The guide will cover a few key basic steps one can take, and then some advanced steps for a higher level of privacy. Basic online security can be achieved in a number of ways. This can include reading privacy policy messages and editing site permissions before allowing access to enter a site. Basic privacy can also be obtained by performing a few key steps.

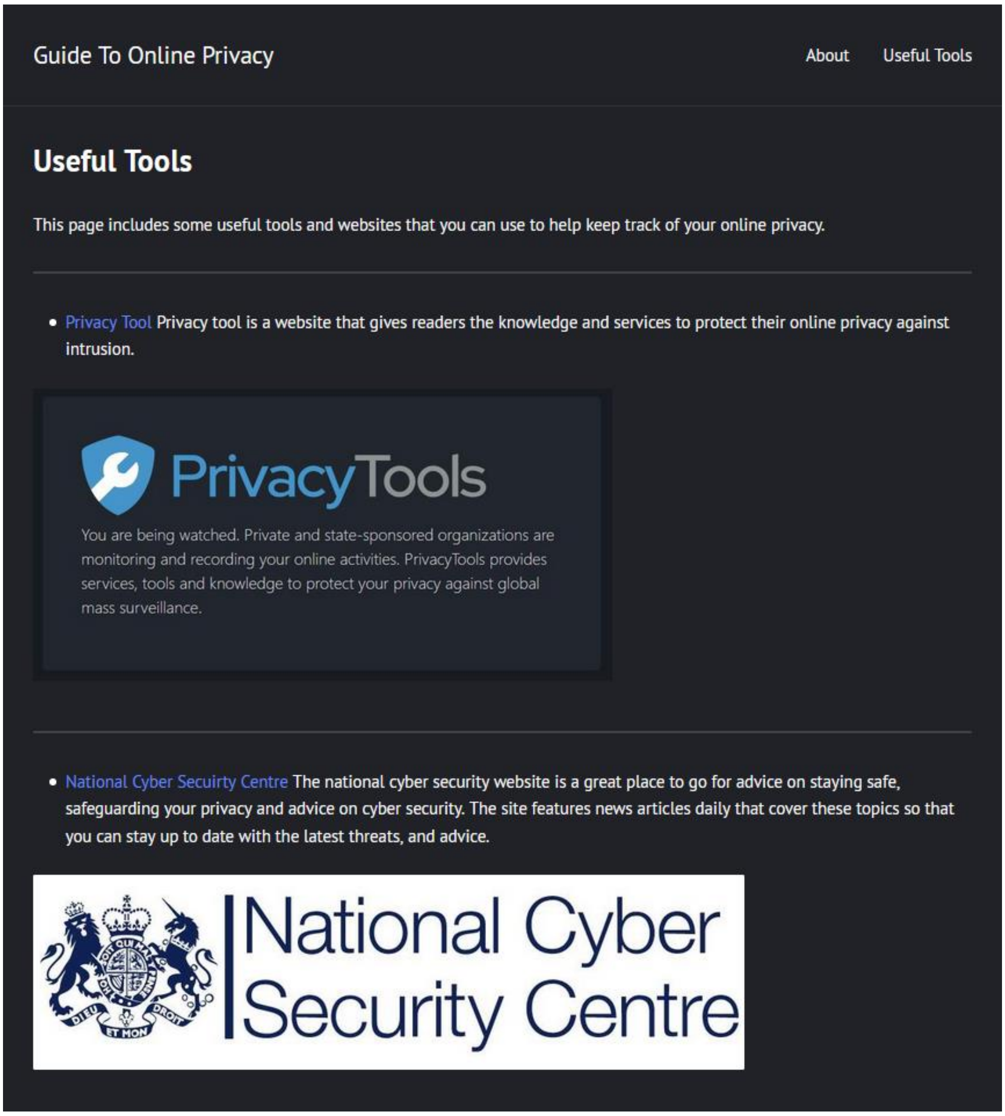
"Google is tracking you on 80% of the top 50,000 websites on the planet"
- Forbes, March 11 2020, John Koesier

The dissertation report can be downloaded here:

Figure 21 - About Page

Useful Tools Page:

The useful tools page provides readers with links to useful tools and sources of information so that they can increase their privacy, and learn more if they want to go further in depth.



Useful Tools

This page includes some useful tools and websites that you can use to help keep track of your online privacy.

- Privacy Tool Privacy tool is a website that gives readers the knowledge and services to protect their online privacy against intrusion.

PrivacyTools

You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. PrivacyTools provides services, tools and knowledge to protect your privacy against global mass surveillance.

- National Cyber Secuirty Centre The national cyber security website is a great place to go for advice on staying safe, safeguarding your privacy and advice on cyber security. The site features news articles daily that cover these topics so that you can stay up to date with the latest threats, and advice.

Figure 22 - Useful Tools page

Chapter 9 – Evaluation:

When looking at the website created, these aims have been met. The website is an easily accessible method of providing information to users, and offers an efficient way of reading about the topic and taking the necessary actions. The website provides easily understood steps that can be taken to safeguard privacy, and pairs it with some useful tools, and images that is packaged together in the website.

After website development had been completed, a few simple questions were asked to users that got to test the completed site.

These questions are as follow:

- Is the design theme, and overall layout of the website good?
- Is the site easy to navigate?
- Is the advice given easy to understand?
- What do you find is the most useful aspect of the site?

- What can be improved?

These question were answered by a few candidates, one aged 19, one 49, and two 22. The responses received to these questions are shown below:

Question one - Is the design theme, and overall layout of the website good?

1. Answer one: Yes the layout is good and appealing
2. Answer two: The layout is nice and minimalistic, very easy on the eyes
3. Answer three: Yes, the design of the site is suited to the content and not over the top like other sites.
4. Answer Four: I think that the look and layout of the page is well designed, but it could use some animations.

Question two - Is the site easy to navigate?

1. Answer one: Yes very easy to use
2. Answer two: Yes the site is good to navigate
3. Answer three: This site is very easy to navigate, its minimalist design make load times very fast and the layout is easy to understand
4. Answer four: Yes this site is simple to use, a 'return to the top of page' button is needed though

Question three – Is the advice given easy to understand?

1. Answer one: Yes, easy to follow
2. Answer two: Yes the advice given is very easy for me to understand
3. Answer three: Yes the advice this site gives is simple to understand and it isn't filled with off-topic information
4. Answer four: Very easy to understand, the links provided are helpful and save time

Question four – What do you find it the most useful aspect of this site?

1. Answer one: The links to other sites for additional info
2. Answer two: The information provided is clear, and easy to understand
3. Answer three: The guide is quick to load and use
4. Answer four: The useful tools page is the best feature

Question five – What can be improved?

1. Answer one: More colour or interactive features
2. Answer two: Some videos would be helpful
3. Answer three: Add buttons to jump to specific pieces of advice
4. Answer four: Welsh language support, there are no good privacy guides offered in welsh.

9.1 - Further improvement:

Based on these responses, the overall reaction to the site is very positive and has provided inspiration for further development and improvements to be made. Firstly there are plans for videos to be added to the site, this adds another form of learning style, and method of providing information to the guide and its readers. This along with the already present feature of alt text for images will allow the site to be used by those with visual impairments more easily. Another feature that is planned is a tutorial page. A tutorial page would provide users with step by step instructions on how to install software, use or change their privacy settings. Including tutorials will help those with low technical knowledge to gain a better level of online privacy without feeling too worried about changing something they should not. Finally, as mentioned in the feedback the addition of the Welsh language will open the website up to a huge market of readers who currently have a lack of easily accessible and useable advice on this topic. The addition of the welsh language or even other languages will make the guide more inclusive, accessible, and useful to many people.

Chapter 10 – Conclusion:

Based on research done on other privacy guides and the results gathered from the survey it is clear to see that the public is interested in their online privacy and ways to safeguard it. This project's aim was to research this topic and create a suitable guide, based on the findings from both primary and secondary research. From these findings it was clear that there is not enough information readily available and understandable to everyday internet users. Creating a website that offered covered these needs and provided them for free to the public was a task that needed to be done.

To conclude; this project was undertaken due to the exponential growth of technology in our lives and the internet of things (IOT – the connection of devices to the internet) This growth brings with it an ever present threat of privacy breaches, but also job opportunities and growth. It is important that privacy is not left behind as an afterthought while using the internet for its many benefits. Users need to be made more aware of the possible threats they could potentially face, and have sufficient knowledge on how to mitigate them. This information needs to be provided in an easy to access, nuanced way that gives the readers all they need to protect their privacy, but also informs them of the sacrifices that sometimes need to be made to do so. The guide created for this project meets this goal. For example, one of the pieces of advice provided states that social media can be a tool used for collecting data privacy breaches, and that this is usually down to the users own actions, while no fault of their own. While social media has opened up many new ground-breaking forms of social interactions and job opportunities, what users post to their feeds matter. A simple photo of your front door or location check-in could lead to an attempted burglary. Reasons like this are just one of many key points that inspired this project to be completed. Although there are improvements and updates to be made to the guide, the overall development and reaction to the site has been very good. The room for improvement means that this site can be further developed and attract a larger audience, some of which have nowhere to go for advice on online privacy. This meets the main objective of this project, to raise awareness of user's online rights, and how to protect their privacy.

Appendices:

Bibliography:

- *(Adam Thierer. (2013). Relax and Learn to Love Big Data. Available: https://www.usnews.com/opinion/blogs/economic-intelligence/2013/09/16/big-data-collection-has-many-benefits-for-internet-users. Last accessed 24/11/20.)*
- *(Audrey Guinchard . (2020). Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? International review of law, computers and technology.*

Available: https://www.tandfonline.com/doi/full/10.1080/13600869.2020.1794569. Last accessed 12/11/10.)

- *(Chris Stokel-Walker. (2020). Universities are using surveillance software to spy on students. Available: https://www.wired.co.uk/article/university-covid-learning-student-monitoring?utm_source=pocket-newtab-global-en-GB. Last accessed 12/11/20.)*
- *(Edward Snowden (2019). Permanent Record. London: Pan Books.)*
- *(ICO Information Commissioners Office (2018). Guide to the General Data Protection Regulation (GDP. London: ICO. Available: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation)*
- *(Martin Giles. (2019). Bounty hunter's tracked people secretly using US phone giants' location data. Available: https://www.technologyreview.com/2019/02/07/137550/bounty-hunters-tracked-people-secretly-using-us-phone-giants-location-data/. Last accessed 10/11/20.)*
- *(William Goddard. (2019). How Do Big Companies Collect Customer Data?. Available: https://itchronicles.com/big-data/how-do-big-companies-collect-customer-data/. Last accessed 22/11/20.)*
- *Home Office. (2020). The Data Protection Act 2018. Available: https://www.gov.uk/government/publications/data-protection-act-national-security-certificates. Last accessed 11/02/21.*
- *Sandra Henshaw. (2019). Identity Theft Statistics: UK & Worldwide Cyber Crime by the Numbers. Available: https://www.tigermobiles.com/faq/identity-theft-statistics/. Last accessed 07.05.21.*
- *Ben Wolford, GDPR EU. What is GDPR, the EU's new data protection law?. Available: https://gdpr.eu/what-is-gdpr/. Last accessed 03.07.21.*
- *Zoe Kleinman - BBC News. (2018). Cambridge Analytica: The story so far. Available: https://www.bbc.co.uk/news/technology-43465968. Last accessed 03.07.21.*
- *Hilary Osborne. (2018). What is Cambridge Analytica? The firm at the centre of Facebook's data breach. Available: https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach. Last accessed 07/03/21.*
- *Jason Fernando. (2021). Cambridge Analytica. Available: https://www.investopedia.com/terms/c/cambridge-analytica.asp. Last accessed 18.04.21.*
- *Matthew Connolly (2018). User Privacy - A Guide for Librarians. : Rowman & Littlefield.*
- *ScienceDirect Authors . (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behaviour. 28, 889-897.*
- *Alexander Maxham - Andriod Headlines. (2020). Google Will Auto-Delete Data It Collects On You – But There's A Catch. Available: https://www.androidheadlines.com/2020/06/google-auto-delete-data. Last accessed 17.04.21.*
- Iulian Gulea. (2018). *The Beginner's Guide To Online Privacy.* Available: https://www.freecodecamp.org/news/the-beginners-guide-to-online-privacy-7149b33c4a3e/. Last accessed April 2021.
- Quincy Larson. (2019). *About freeCodeCamp - Frequently Asked Questions.* Available: https://www.freecodecamp.org/news/about/. Last accessed 18.04.21.
- Quincy Larson. (2017). *How to get published in the freeCodeCamp Medium publication.* Available: https://www.freecodecamp.org/news/how-to-get-published-in-the-freecodecamp-medium-publication-9b342a22400e/#.7zth1t3qa. Last accessed 19.04.21.

- Ludovic Rembert. (2021). *Online Privacy: 11 Ways To Protect Yourself in 2021 (and Beyond).* Available: https://privacycanada.net/online-privacy-guide/. Last accessed 19.04.21.
- Jade Dominguez. (2013). *How Jekyll Works.* Available: http://jekyllbootstrap.com/lessons/jekyll-introduction.html. Last accessed 20.04.21.

LSEPI (Legal, Social, Ethical, and Professional Issues):

I have briefly covered and described the legal issues, GDPR (2016) and the freedom of information act (2000) as they relate to the report subject. I have not interpreted these laws in my own way or gave my opinion on them. I have just covered the relevant parts and described them in as clear and easy to understand way as possible, so that the reader has an understanding of its meaning and effects. As stated in my ethics sheet, my dissertation topic does not risk running into any ethical or legal issues. I have set the survey so that all answers form the public are completely anonymous, and I have covered this in the intro section of the survey. The intro states: "This survey aims to collect data regarding people's experiences and habits in relation to online privacy. Data will be analysed and used in my dissertation "An investigation into how engaged people are in online privacy issues, are they aware of their rights, how data is taken, and how to prevent it". All data collected will be completely anonymous. Thanks for taking the time to complete the survey." The questions in the survey are mainly focused on the readers' knowledge on the subject, their opinion on these topics, and what can be done to improve things. None of these questions are unprofessional, un-ethical, and all answers have been recorded anonymously so there are no legal issues that I need to cover. I have not used any software that requires a license to use, and all software I have used is completely free to use and accessed online. My report is written as an investigation and a guide, my own personal opinion on the topics has not been used and any mention of my own opinions, such as different methods on how best to protect your data, it will be clearly stated. I have investigated and made sure that any sources I have used are from credible places, and that they use or base their opinion off of credible evidence.

Legal:

For the primary research conducted in this report, a simple online survey is utilised. This survey collects no personal user data such as names, contact information etc. to ensure anonymity. Research conducted for this report also covers internet laws such as GDPR. All information used is taken from the UK GDPR guidance document, and is not reinterpreted. The "guide to online privacy" website does not make use of any cookies, store information, or the use of copyrighted material. All material used is original, or taken from copy right, free to use sources, and is a simple source of information. It is clearly stated that all advice given on the website is unprofessional, and is a guide on the steps readers can take to increase their online privacy based on research.

Social:

The online survey that is used in this project was done anonymously, and recorded zero data on the responders. The survey was not answered by anyone under the age of 18, and did not feature any controversial or otherwise inappropriate or irrelevant questions. The website is designed to be easily navigated, and the advice given is easily read and understood. This is done by making use of a minimalist design choice for ease of navigation and fast load times. The advice given is written so that it is jargon free and can be read by those with little to no technical knowledge.

Ethical:

The report is nuanced, opinion free, and used reliable sources of information so that it is ethical when making points. The primary research was conducted in an ethical way, and shared in the form of email, and social media sharing. All questions asked are relevant to the topic and suitable for its target audience. The website features content that is relevant and suitable to its target audience, and is conveyed in a number of different ways. The guide was developed with different learning styles in mind, and is suitable for those with disabilities such as loss of sight or hearing. The advice given in the guide is advice that is based on research, my own experience, and informs the reader of what will happen if they follow the advice. The website states that all advice given is to be taken by the reader on their own accord, and they should weigh the pros and cons of following the advice personally. It is also stated on the website that the advice given within the guide is merely steps that can be taken to increase online privacy, is accurate at the time of writing, and is not professional.

Professional:

As stated above the primary research conducted in the form of an online survey, is 100% anonymous and no personal data is collected. All questions asked in the survey are appropriate, meet the target audience, and are professional. Where the report has made use of research such as statistics, or quotes, the information is used and conveyed in a fair, nuanced, unchanged, and professional manner to provide context and state facts rather than opinion. All sources of information used are also referenced in the Harvard style. Content used on the website such as the Jekyll theme are copyright free and free to use. The ‘useful tools’ page on the website features links to tools or websites that can be used to greater increase the level of awareness the user has of their privacy. These links have been picked to be suitable for the target audience, relevant, and free to use.