

# SOLENT UNIVERSITY

---

SOUTHAMPTON

*Faculty of Business, Law and Digital Technologies*

**MSc Cyber Security Engineering**

**September 2022**

**Edward Nevard / Q14161940**

**Dissertation**

**Research Project (MAA112) – AE1**

**Is resilience engineering achievable in the age of Big Tech dependency?**

## **ABSTRACT**

The world has become saturated with Big Tech dominance. Google answers 92% of the world's search queries, >50% of all e-commerce goes through Amazon and over 70% of internet referral traffic goes via sites owned and/or operated by Google and Facebook. Big Tech is causing long-lasting damage to young people's mental health, continues to jeopardise national and civil cyber security through intrusive data collection, bankrupts and acquires smaller businesses, monopolises our digital communication avenues and remains a huge risk to our digital and physical worlds. Yet, as a society, we have become completely dependent and entrusting on these five companies to continue operating large parts of our lives. This thesis explores the alternative solutions to dependency on Big Tech products and services, and investigates why the situation has gotten so serious, so quickly.

Accompanying the research are two practical projects, both of which further explore our dependency on Big Tech within our daily lives, by using a case study analysis of people with multiple age groups and professions using a network in which Big Tech is no longer accessible from the rest of the internet.

## ACKNOWLEDGEMENTS

---

Firstly, I would like to thank my tutor, **Dr Andy Farnell**, for his outstanding commitment to both me personally, and my project, throughout the past year. His support and guidance have ensured my continued success, and I will be forever grateful for this. His passion and courtesy towards all his students and subjects are unmatched.

---

Secondly, I would like to thank my remarkable Mum, **Yvonne Nevard MA, BA (Hons)**, for being the most supportive parent that I could ever ask for, especially in this last year. You're one of the strongest people I know, and I would not be writing this without your support.

---

Thirdly, I would like to thank my cohort, tutors, and the Mental Health Team at Solent University, as well as my incredible friends and family for their support and motivation throughout what has been the hardest year of my life, for several reasons. I could not have gotten this far alone. To name just a few:

- **Henry & Josephine Nevard**
  - **Anita & Andy Hacking**
    - **Anthony Fulker**
  - **Bev, Gillian & the late Malcolm Irving**
  - **Darrell Dwayne van den Bos**
  - **Donna Saunders BA (Hons)**
  - **Helen Plews BA (Hons)**
  - **Joe Grant BSc (Hons)**
    - **Ken Tyre**
    - **Stacy Dunn**
    - **Stetson Blake**
- 

Finally, I want to pay tribute to several family members that have left this world much sooner than they should have in recent years:

- ◆ My Dad, **Justin Nevard**, who passed away suddenly in July 2021 at the age of 51 – a few months before I was due to begin my master's degree. I wouldn't be where I am today without your support and guidance and your passion for IT. There's nothing I wouldn't give to see your reaction after telling you I've completed my master's degree. You were in my thoughts at every step along the way, and always will be.
  - ◆ My Uncle, **Laurence Nevard**, who passed away suddenly in December 2018 at the age of 53. You have left me with so many happy memories that have inspired me to keep going, even in life's hardest moments. You were such a hard worker and aspire to have a successful career in the industry like yours.
  - ◆ My Grandad, **Allen Saunders**, who left us in May 2022 (this year) at the age of 82 after a short battle with cancer. Your ability to find positivity in the most challenging moments of life have helped me re-evaluate how I think. Even in the toughest scenarios, I still hear your voice of reason championing me along.
-

## A DEDICATION

---

This thesis is dedicated to all those who have experienced adverse, prolonged, or permanent effects as a direct result from the continued behaviour and actions of Big Tech, which has found itself deeply ingrained within almost every element of our society.

With an immeasurable number of teenage lives lost, millions who are struggling with mental health conditions due to social media and mobile technology abuse, countless independent businesses and livelihoods destroyed, and an epidemic of social and economic issues caused by the behaviour of a few companies, I apologise to all these people on behalf of our society. I am sorry, we should have, and need to, do more about it.

I strongly believe this is amongst some of the biggest failings of history, and whilst we are beginning to turn a corner now, we have a lot further to go.

## ACRONYMS

Acronym	Description
ASN	Autonomous System Number
BGP	Boarder Gateway Protocol
Big Tech / Big Five	Alphabet (Google), Amazon, Apple, Meta (Facebook) & Microsoft
CDN	Content Delivery Network
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSS	Cascading Style Sheet
DNS	Domain Name System
EU	European Union
FLoC	Federated Learning of Cohorts
FreeBSD	Unix-like OS based on Berkeley Software Distribution Unix
HTML	Hyper Text Markup Language
I/O	Input/Output
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
JS	JavaScript
LAN	Local Area Network
LTD	Top-Level Domain
NIC	Network Interface Card
NPM	Node Package Manager
OSI	Open Systems Interconnection
PC	Personal Computer
RAM	Random Access Memory
SaaS	Software as a Service
URL	Uniform Resource Locators
VPN	Virtual Private Network

## TABLE OF CONTENTS

Abstract.....	1
Acknowledgements.....	2
A Dedication.....	3
Acronyms .....	4
Table of Contents.....	5
Table of Figures.....	8
Table of Tables .....	9
1. Introduction .....	10
2. Background .....	12
2.1. Ongoing Legal Challenges .....	12
2.2. Why Organisations are ditching On-Premises for Cloud .....	13
2.3. Risks surrounding Big Tech Dependency / Cloud.....	14
2.4. Real-world Case Studies of Cloud Issues.....	15
2.5. Adblocking, Anti-advertising & Anti-Tracking Culture .....	16
3. Methodologies .....	17
3.1. Methodology Scope .....	17
3.2. Modern Deliverable Structure of Web Pages .....	17
3.3. Practical Scenarios .....	18
3.4. Scenario A – Total Disconnection .....	18
3.5. Scenario B – Selective Disconnection .....	18
3.6. Firewall Appliance Explanation .....	19
3.7. Use Case Applications .....	20
4. Preliminary Research Results.....	21
4.1. User Classes .....	21
4.2. Survey.....	22
5. Practical Projects.....	30
5.1. pfSense Layer 3/4 Blocking .....	30
5.1.1. Background & Pre-Setup.....	30
5.1.1.1 Why PfSense?.....	30
5.1.1.2 Acquiring Hardware .....	30
5.1.1.3 Installation Process .....	31
5.1.2. Logical Functionality & Visual Configuration .....	31
5.1.2.1 Firewall Functionality in Depth .....	31
5.1.2.2 Network Topologies .....	34

5.1.3.	Creation of Rules.....	35
5.1.4.	Testing.....	37
5.1.4.1	Initial Functionality Testing.....	37
5.1.4.2	Key User Scenario Testing & Analysis (Results) .....	38
5.1.5.	Concluding Project Comments.....	41
5.2.	Is It Big Tech Website (isitbig.tech).....	42
5.2.1	Background & Pre-Setup.....	42
5.2.1.1	Puppeteer – the high-level Chromium API .....	42
5.2.1.2	Web Server Configuration.....	42
5.2.1.3	Development & Hosting Environment.....	43
5.2.2	Logical Funcationality.....	45
5.2.2.1	Logical Process Representation .....	45
4.2.1.1	File & Folder Structure .....	45
5.2.3	Brief Essential Code Explanation.....	46
5.2.3.1	Index.js .....	46
5.2.3.2	/src/big_data.js .....	47
5.2.3.3	/src/puppeteer.js .....	48
5.2.4	Public Viewable Pages.....	49
5.2.4.1	Index (Home).....	49
5.2.4.2	About.....	49
5.2.5	Testing.....	50
6.	Mitigations & Recommendations .....	53
6.1.	Legal Measures .....	53
6.1.1.	Force Majeure .....	53
6.1.2.	Legislators & Regulators .....	54
6.1.3.	Exising Legal Inadvertance .....	55
6.2.	Adaptability & Resillience .....	56
6.2.1.	Resilience – The Customer/Consumer responsibility? .....	56
6.2.2.	The Four Rs.....	56
6.2.2.1.	Refuse.....	57
6.2.2.2.	Reduce.....	57
6.2.2.3.	Reuse.....	57
6.2.2.4.	Recycle .....	57
6.2.3.	Killer Acquisitions.....	57
6.2.4.	Defence from Future Harm.....	57
6.3.	Education .....	58

6.3.1.	Arrival through Poor Education .....	58
6.3.2.	Productization .....	58
6.3.3.	Polarised and Monopolistic Market.....	59
6.3.4.	Organisational Intervention .....	59
6.3.5.	The Tech Sector & Developers.....	59
6.3.6.	The Next Generations .....	60
6.4.	“Mr Robot” Scenarios .....	61
6.4.1.	Scenario One — Inevitable Failures .....	61
6.4.2.	Scenario Two — Government/Political Involvement of Big Tech.....	62
6.4.3.	Scenario Three — Self-Devourment .....	63
7.	Conclusions .....	65
7.1.	Preliminary Survey Conclusions .....	65
7.2.	Awareness Through Education and Messaging .....	65
7.3.	Current Viable Technologies & Actionable Mitigations.....	65
7.4.	Legislative Implementation Concerns.....	66
7.4.1.	3 Stages of Correction.....	66
7.4.1.1.	Stage 1 – Popular Awareness.....	67
7.4.1.2.	Stage 2 – Think Tanks, Advisory Boards & Individuals.....	67
7.4.1.3.	Stage 3 – Implement Legislative Change .....	67
7.4.2.	Short-Termism is The Enemy .....	67
7.5.	Future Research .....	67
8.	Further Reading .....	68
	Digital Resilience Framework – UK Council for Internet Safety (UKCIS_Digital_Resilience_Framework.pdf (publishing.service.gov.uk) .....	68
	Digital Vegan by Dr Andy Farnell .....	68
	Don't Be Evil: The Case Against Big Tech by Rana Foroohar.....	68
	Ledger of Harms – Center for Humane Technology ( <a href="https://ledger.humanetech.com">https://ledger.humanetech.com</a> ).....	68
	Open-Source Alternative ( <a href="https://www.opensourcealternative.to">https://www.opensourcealternative.to</a> ) .....	68
	Resilience in the Digital Age by Fred S. Roberts, Igor A. Sheremet .....	68
	System Error: Where Big Tech Went Wrong and How We Can Reboot by Rob Reich .....	68
9.	References .....	69
10.	Appendix A – Letters to Organisations .....	75
	DuckDuckGo.....	75
	Secretary of State for Education.....	76
11.	Appendix B – Big Tech Acquisitions .....	78
	Amazon .....	78

Apple .....	80
Facebook (Meta) .....	82
Google .....	83

**Note: Sections 1, 2-2.4, 3, 4 and 7.1 have been imported from my Pilot Study submissions.**

## TABLE OF FIGURES

Figure 1: Typical Web Page Structure .....	18
Figure 2: Example Standard Unprotected Consumer Network [Logical Representation] .....	19
Figure 3: Example PfSense Filtered Traffic Network [Logical Representation] .....	20
Figure 4: Big Tech Use Cases Table .....	21
Figure 5: Preliminary Survey Q01 .....	22
Figure 6: Preliminary Survey Q02 .....	23
Figure 7: Preliminary Survey Q03 .....	24
Figure 8: Preliminary Survey Q04 .....	25
Figure 9: Preliminary Survey Q05 .....	26
Figure 10: Preliminary Survey Q06 .....	27
Figure 11: Preliminary Survey Q07 .....	28
Figure 12: Preliminary Survey Q08 .....	29
Figure 13: pfSense Hardware .....	31
Figure 14: PfSense Install Process .....	31
Figure 15: PfSense WHOIS AS Request .....	32
Figure 16: PfSense Data Flow AS Block Check Process .....	33
Figure 17: Four Layers of TCP/IP Model (Williams, 2022) .....	33
Figure 18: Wider Logical Network Topology .....	34
Figure 19: Focused Network Topology .....	35
Figure 20: ASN Firewall Rule Creation .....	35
Figure 21: Completed ASN Block List Rules (Big Tech) .....	36
Figure 22: PfBlocker-NG IPv4 Setup Process Logs .....	36
Figure 23: pfBlockerNG ASN Packet Statistics .....	37
Figure 24: Hardware Usage (Idle vs Big Tech Traffic) .....	37
Figure 25: Windows 11 System Crash .....	37
Figure 26: Nginx Proxy Basic Configuration (/etc/nginx/sites-enabled/default) .....	42
Figure 27: Nginx Proxy SSL Certbot Configuration (/etc/nginx/sites-enabled/default) .....	43
Figure 28: PM2 Status Output .....	43
Figure 29: IsItBigTech Git Commits .....	44
Figure 30: Website Logical Process Representation .....	45
Figure 31: IsItBigTech Application File & Folder Structure .....	45
Figure 32: IsItBigTech - index.js .....	46
Figure 33: IsItBigTech - /src/big_data.js .....	47
Figure 34: IsItBigTech - /src/puppeteer.js .....	48
Figure 35: IsItBigTech - Index (Home) .....	49
Figure 36: IsItBigTech - About .....	49
Figure 37: The 4 Rs .....	56
Figure 38: 3 Stages of Correction .....	66



Figure 39: Email to DuckDuckGo.....	75
Figure 40: Email to Secretary of State for Education.....	76
Figure 41: Reply from Department for Education .....	77

## TABLE OF TABLES

Table 1: PfSense Hardware Specifications.....	30
Table 2: Disconnection and Reliability Type Scale Key .....	38
Table 3: User Affectability – Disconnection and Reliability Experiment.....	41
Table 4: IsItBigTech Site Dependency Testing .....	52
Table 5: Big Tech Fines.....	63
Table 6: Big Tech Acquisitions - Amazon .....	79
Table 7: Big Tech Acquisitions - Apple .....	81
Table 8: Big Tech Acquisitions – Facebook (Meta).....	83
Table 9: Big Tech Acquisitions - Google .....	86

## 1. INTRODUCTION

Organisations and individuals across the globe are handing over full responsibility of their digital footprint to Big Tech companies daily, with a continuous drive to retire on-premises equipment and their engineers in exchange for cloud services, in a bid to lower running costs and reduce complexity of their general operations. From this point of view, especially for small businesses, it is understandable why this change seems positive and instantaneously beneficial. This is the start of a problematic cycle.

The term 'Big Tech' is used to represent the most dominant and prestigious technology firms in the world (Financial Times, 2022), also currently known as the 'Big Five', which are: Alphabet (Google), Amazon, Apple, Meta (Facebook) and Microsoft.

In 2021, they crossed a combined revenue of over \$1.4 Trillion (Muhammad, 2022), and the total worth of the combined giants is around \$8.4 Trillion (Wilhelm 2021), which raises several questions around how these companies earn their money and where it is invested, especially in recent years (Ovide, 2021).

To put into perspective the amount of capital this is, if these Big Five companies formed a nation state, they would become the third richest country in the world, surpassing huge economies such as Japan (\$4.87tn), Germany (\$3.69tn), India (\$2.65tn), United Kingdom (\$2.63tn), etc (worldometer, 2017).

This vast amount of capital occupied by the giants alone, in turn, gives them immense amounts of political and social power (more than most national governments). In addition, individuals and smaller firms are continuing to willingly feed the Big Tech firms with their money and data, causing them to grow more than any known organisation in the world to date and monopolising the flows of information and communication.

Big Tech have caused / are continuing to cause grave harm to many sectors of people's lives, all over the world, from Facebook diminishing and manipulating our democracies through targeting campaigns at users using very intimate and targeted datapoints to twist their views (Cambridge Analytica scandal (Wong, 2019) as a prime example), Amazon bankrupting our high streets through unfair competitive pricing on an unbeatable scale for smaller shops due to their huge purchasing capabilities (Greenfield, 2021), and the majority of educational and government establishments now using Big Tech cloud-based platforms such as Google Workspace and Microsoft Office 365 with 97.9% of the market share between them in 2018 (Joe, 2021), monopolising the entire market. A recent and concerning example is the award of a cloud contract to Amazon to host classified material for GCHQ, MI5 & MI6 (Syal, 2021).

Whilst Big Tech monopolies are the 'sun and centre' of an ever-expanding tech universe and the problems this brings, it is not necessarily the Big Five that are the main problem. It is the misplaced trust from individuals and smaller companies that are willingly handing over their money and digital property to them, in essence, feeding the monopoly machine and contributing to the continued growth and inadvertently becoming a subsidiary or "estate" of the Big Tech provider – which is a catastrophe.

The attempts made to regulate and/or interrogate Big Tech firms even by the biggest economic powerhouse in the world, the United States, the very birthplace of the Big Five, have continuously fallen short of useful, majorly due to the lack of understanding by politicians and congresspeople of the issues at large.

The European Union are offering the most promising potential with the regulation of Big Tech, after constructing a new law to reduce Big Tech dominance, although this is mostly in the consumer choice and mobile application aspects of the problems, and curbing the “buy and kill” mentality, acquiring competition companies, which has been the case for decades (Waters, 2020).

This thesis will explore in depth the ongoing issues with the ever-growing dependency on Big Tech companies and their cloud services, the long-lasting effects on businesses, and the effects on the general consumer.

The accompanying project will explore how much of the browsable internet is left “usable” by a general user from a firewalled Local Area Network, with rules in place to block all domains/IP address ranges owned by Big Tech firms, exploring the wider footprint of the Big Five, how affected many unsuspecting websites and applications are by the blocks, and the level of disengagement experienced by users without the presence of their services, such as content delivery networks (CDNs).

Continued uptime is vital to any organisation and Big Tech cloud hosting is very well established, packaged with many mitigation and backup features, such as geographical data backups, datacentres in multiple territories, etc. This is, of course, a substantial benefit to using cloud services. Uptime/usability is a consideration that needs to be made within the risk assessment of engineering a future without the central reliance on Big Tech services, no matter the size of the organisation, which can seem precarious when re-introducing on premises services, though there are ways to mitigate risk.

Leading to the all-important question, is resilience engineering achievable in the age of Big Tech dependency?

## 2. BACKGROUND

### 2.1. ONGOING LEGAL CHALLENGES

Big Tech have faced and are continuing to face a variety of legal challenges, mainly within the European Union currently.

Until very recently with the EU's legislative action with their Digital Markets Act, many legal systems haven't had the mental capacity to understand what is happening around the technology space, with outdated laws that do not cover the global issues surrounding the monopoly that is Big Tech. This was proven from the attempts made by the United States congress in recent years as mentioned previously, which shows their clear disassociation from the real issues that are caused by Big Tech.

There is speculation in Europe from both the governments and citizens on whether to split up these Big Tech companies, and whilst it is easy to understand this sentiment, it is proving their lack of consideration with the situation given the number of subsidiary companies that are already owned by Big Tech – this would contribute to this situation in a negative way, essentially splitting the same company up into smaller elements and making their overall activity harder to track and causing impractical market fragmentation. For example, if the government broke up a company like Tesco into smaller shops, but with different names, it could produce an illusion of choice to consumers whilst realistically, it is the same company.

The Digital Markets Act promises to put an end to unfair business practices, obligations, and prohibitions directly applicable to “gatekeepers” of the market, restrictions on “killer acquisitions” and minimum fines of 4% up to 20% for any failure to comply with the new legislation (European Parliament, 2021). This is a huge step forward and proves that the EU are becoming aware of the power that these digital giants have, with a closing statement in their press release, “Our message is clear: the EU will enforce the rules of the social market economy also in the digital sphere, and this means that lawmakers dictate the rules of competition, not digital giants” (European Parliament, 2021). Whilst there is much more work to be done, and some questionable contents of the act, the legislation does provide a light at the end of the very deep and dark tunnel that has been the Big Tech monopoly for years, strangely one that many consumers haven't realised they have been in.

The recent attempts to interrogate the Big Tech CEOs at their congressional hearings in the United States is both comical and disconcerting in regards to the level of attentiveness the Congresspeople seem to stipulate through their shockingly out-of-touch questions, such as (in address to Mark Zuckerberg) “If I'm emailing within WhatsApp, does that ever inform your advertisers?” and “Can somebody call you up and say I want to see John Kennedy's file?” (CNET, 2018).

The EU are certainly the leaders in the legal battles to finally curb the dominance caused by Big Tech, and the hope is that the rest of the world will follow in suit.

## **2.2. WHY ORGANISATIONS ARE DITCHING ON-PREMISES FOR CLOUD**

There are a range of reasons for organisations ditching on-premises systems in exchange for cloud services, mainly for the increased reliability, reduced responsibility, and less maintenance costs across their infrastructure, which are of course, hugely beneficial and enticing benefits, especially to smaller businesses, and even more so in recent years with the continuing rise in electric prices and the ongoing microchip shortage (James, 2022).

As the Big Five largely dominate the market share of cloud services, they price many cloud providers out of the market, offering much lower costs for the same product due to their ability to get better deals with datacentre wholesale costs, in both energy, construction and systems.

With on premises systems, the company is responsible for the maintenance, computer systems, and other infrastructure needed to support the solution. In addition to this, there is also increased cost for in-house IT staff which are required to support, maintain, and troubleshoot any issues. This is a huge cost, especially for smaller businesses who cannot expend that amount of money with tight profit margins. With cloud services, only the resources used are paid for, and responsibility of all maintenance and server failures are down to the provider to fix as the hardware and network is owned by the provider – therefore they swallow the cost of any dysfunctional equipment. Cloud computing is 40x cost-effective compared to on premise IT systems for small to medium businesses. (Bulao, 2022)

To scale on premises systems, access to manual labour, hardware and software will determine how able a business is to do this. Scalability is generally easier using cloud services, with flexibility for sudden surges in activity and increased demand over time, allowing growth with a business on a pay-as-you-go basis.

The COVID-19 pandemic rapidly accelerated the adoption of cloud-based infrastructure, with remote work becoming a “new normal”, companies had to ensure they were able to support and provide critical services to their off-site workforces (Checkpoint, 2022).

It is estimated that the cloud computing market will be worth \$800 billion by 2025 and by 2024, enterprise cloud spending will make up 14% of IT revenue globally.

In 2020, Amazon Web Services had a 76% share of the enterprise cloud adoption. At the same time, it was found that the UK was the third-largest cloud consumer in the world, spending \$13.8 billion in 2020, with the United States in first place at \$171 billion.

### **2.3. RISKS SURROUNDING BIG TECH DEPENDENCY / CLOUD**

Reliance on someone else's systems of course never comes without risk, no matter how well established or how much funding is behind the continued running and development of the infrastructure, failure can still occur.

Arguably, the biggest disadvantage is complete loss of control and visibility to the systems. When an organisation moves their services to the cloud, they are handing over their data and information. Even if a company has in-house IT staff, they will not be able to handle any complications on their own – for example, in the event of a hardware failure or a cyber-attack on the cloud infrastructure, or network outages (O'Donnell, 2020)

Cloud providers are generally a bigger target for potential hackers due to the potential payoffs of a successful attack, and even if businesses assets are encrypted within the platform, they are still at risk of heavy downtime and loss of income, depending on the business. There have been many publicised cloud breaches, especially in recent years, and theft of personal information to intellectual property prove to be very real threats.

If there are any IT staff in house, the move to cloud providers involves retraining and will always come with increased complexity strains. Skilled engineers will also be limited by the access the cloud providers offer to the business once they have migrated their systems.

Due diligence is also something that many organisations (especially smaller businesses) do not always carry out as thoroughly as they should, which can pose significant cyber security risks when choosing a cloud provider and their services. This can have an impact on their data privacy and compliance, depending on where the systems are hosted and lack of international standards implementation within the business. Some essential considerations that need to be made are the incident response procedures on both the provider end and the organisation/individual themselves, who is responsible for data encryption, and who is monitoring the security on both ends, and how? (Spanning, 2013).

Ultimately, the reliability of data or services hosted by cloud providers is out of the control of the customer, and if any outages/breaches occur, the business can grind to a halt.

## 2.4. REAL-WORLD CASE STUDIES OF CLOUD ISSUES

Although Big Tech invest a lot of money into the continued development and cyber security of their cloud systems, they remain prime targets for potential hacking attempts due to the extensive rewards that could be gained from a successful attack, including source code leaks, customer details, etc. With companies like Amazon Web Services now hosting classified data for intelligence agencies such as GCSQ, MI5 and MI6 (Syal, 2021) and hosting some of the biggest tech companies in the world, such as Netflix, Facebook, BBC, Adobe, and Twitter (Gillard, 2020), it is no wonder why these cloud platforms are becoming bigger targets for potential attacks by the day. According to a report by IT Governance, 5.1 billion records were breached in 2021, with 1,243 reported incidents, with an 11% increase in attacks compared to the previous year with 1,120 in 2020. Across all four quarters of 2021, cyber-attacks were the leading security incident (Irwin, 2022).

With so many companies being hosted in a monopolised cloud market, outages have a huge widespread effect on the internet. Just last year in 2021, Amazon Web Services suffered three outages within three weeks, one lasting 7 hours before it was fixed. All amazon “smart” devices such as Alexa and ring cameras, IoT cat feeders (they stopped working completely due to reliance on Amazon Web Services), prime video, and others were rendered useless due to the outage, as well as third-party applications like Disney+ and Facebook suffered outages because of their choice in cloud provider (Sutrich, 2021).

In 2021, Ubiquiti suffered a substantial breach of their systems which exposed customer account credentials. A whistle-blower later reported that the company massively downplayed a “catastrophic” incident to minimise the hit to its stock price. The hackers obtained full read and write access to their databases hosted by Amazon Web Services (Nevard, 2021).

In April 2021, Facebook reported a breach which affected over 533 million user records, publicly exposed on Amazon’s AWS platform. Two third-party Facebook app development companies posted the records in plain sight. The database contained private information that could be used in social engineering, hacking or fraud attempts. The exposed data included 32 million records on users in the United States and 11 million users in the United Kingdom (Holmes, 2021).

Earlier this year, a ransomware hacker group named Lapsus\$ were reported to have breached internal source code repositories for Microsoft Azure DevOps as they published a photo allegedly from a Microsoft server, showing access to Bing and Cortana-related projects. A Microsoft spokesperson stated that “we plan our security with an assume breach philosophy and layer an in defence-in-depth protections to controls and stop attacks sooner when they do gain access” (Millward, 2022).

## 2.5. ADBLOCKING, ANTI-ADVERTISING & ANTI-TRACKING CULTURE

Big Tech dominance has affected consumers/general users for a lot longer than businesses, though. Adblock, the browser extension, now available for most major browsers, was launched back in December 2009. This, obviously, did not have good effects on companies who were beginning to make a lot of money from tracking and advertisements as the internet began to grow exponentially – especially with internet-connected smartphones becoming mainstream after the release of the iPhone 3GS in June 2009 (Apple, 2009).

In a New York Times article shortly after the release of Adblock, it stated that Jonathan Rosenberg, the senior vice president for product management at the time, emailed all Google employees to inform them to commit to “greater transparency and open industry standards” (The article then goes on to mention that Google’s inclusive principles “are being put to the test” due to this ongoing situation. (Cohen, 2010). Rosenberg later resigned from Google in 2011, two years earlier than originally planned (Guynn, 2011). This is just one historical example of the motivations of ordinary people who wanted to put some form of resilience against them and intrusive Big Tech advertisements, which has now grown into one of the most downloaded browser addons within the Google Chrome Web Store. Google does not publish the exact number of downloads, but at the time of writing, it is displayed as “10,000,000+ users”. According to Kratky-Katz (2021), the 2021 PageFair Adblock Report highlights some important statistics. It states that mobile adblocking grew 10% to reach 586 million users, and desktop adblocking grew 8% to reach 257 million users.

In June 2015, the Pi-hole® open-source project was released by Jacob Salmela (Salmela, 2015). Pi Hole is what is known as a DNS Sinkhole, which can be deployed on a private network on almost any Linux computer, including support for ARM (Initially released for use intended on a Raspberry Pi, hence the project name) & x68 architectures. The main goal of the project is to block DNS requests for known advertisement and tracking domains from communicating with any devices on the network that have their DNS server set as the PiHole, preventing the malicious traffic from accessing the network. This project has grown immensely since its initial release in 2015, with many contributors working to keep tracking/ad lists up to date daily (currently 210 on its GitHub repository), (pi-hole, 2022), and is one of the leading and most well-known projects for anti-tracking.

Browser cookies were invented by Lou Montulli in 1994 for Netscape, to identify users accessing a web store, noting regular customers, finding out whether visitors are mostly tourists or locals and likely buyers or just browsers. Before the use of cookies, visitors to websites were anonymous web users with no way of being individually identified (Singleton, 2000). There was a lot of retaliation even at the time of release because of this reason, “Cookies have taken a lot of heat since they were introduced earlier this year. That’s because they seem to remove one of the great features (or problems) of the Web: anonymity” (Garfinkel, 1996). Fast forward to 2022 and the death of third-party “evil” cookies (and therefore tracking they are used for) is upon us. Browsers are already preventing third-party cookies by default, which is good news for the average user. This is what has been the rock on which the independent online advertising businesses and will have catastrophic consequences for them – but not the Big Five – it won’t eliminate first-party and second-party cookies, “While independent ad tech companies will struggle to target their advertisements effectively, the biggest companies sit atop a wealth of owned data resources and sophisticated targeting tools.” (Slager, 2022). Overall, leaving yet another stacked deck for Big Tech – Google are already working on replacement solutions such as FLoC, which have been met with total resistance, “Several web browsers (Firefox, Brave, Vivaldi, and Opera) announced they would not support FLoC in its current form because it fails to provide sufficient user privacy.”, “DuckDuckGo, rejected it outright” (WNIP, 2021). Anti-tracking and advertising culture is certainly not going to diminish.



### **3. METHODOLOGIES**

#### **3.1. METHODOLOGY SCOPE**

To determine the level of dominance that the Big Five hold across the usable internet, and the amount of dependency that people have on their services, a scenario must be created in which these services are no longer accessible in order to access primary quantitative data for analysis.

The practical application will involve scenarios in which Big Tech services are disconnected to a lab-environment LAN behind a physical PfSense Firewall:

- Scenario A is complete disconnection (by blocking entire DNS and IP address blocks) from Big Tech servers and domain names.
- Scenario B aims to deliver as much functionality as possible, but without the high levels of tracking, advertisements and unwanted malicious content delivered by these services.

The clients within this LAN will then be assessed to see how much of the usual internet browsing becomes interrupted, especially on websites and applications that are not directly linked to the Big Five but rely on their services to deliver this content to the client, such as Content Delivery Networks (CDNs) hosted by Amazon Web Services or Microsoft Azure, for example.

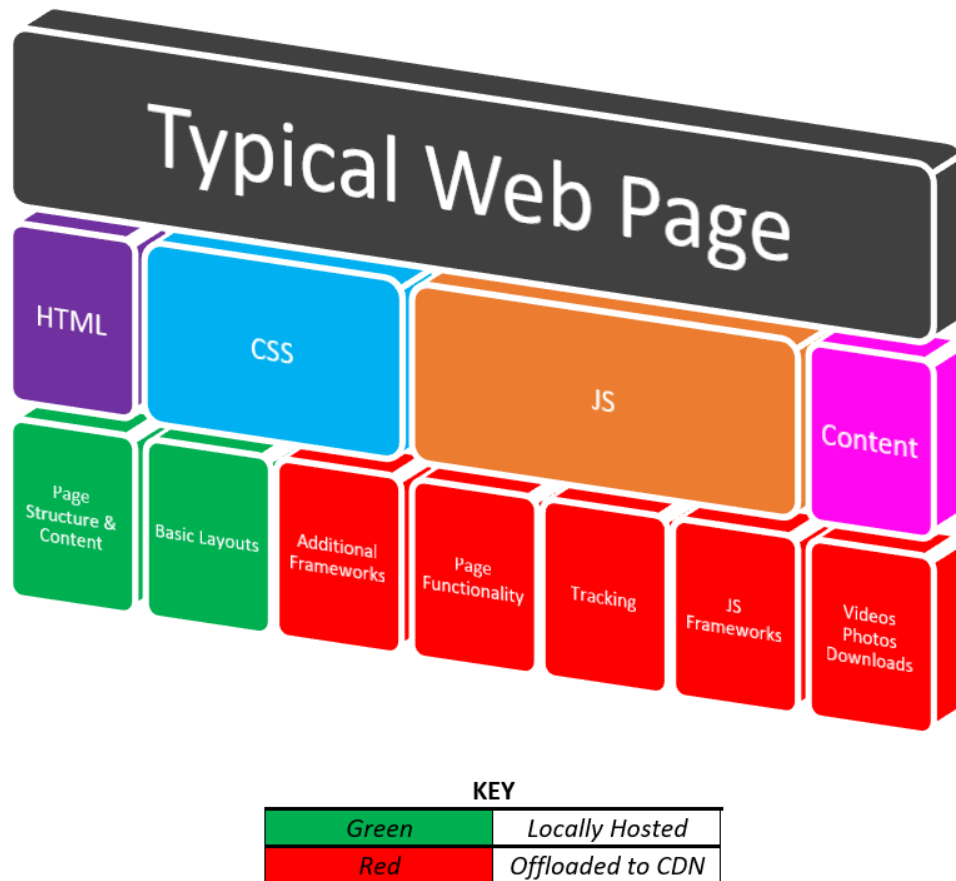
Alongside the “usual internet browsing”, functionality of devices that rely on Big Tech services to operate will also be assessed. For example, OTA (Over the Air) software updates, applications, etc.

#### **3.2. MODERN DELIVERABLE STRUCTURE OF WEB PAGES**

CDNs are a network of servers that deliver web content to end users. CDN's are used by companies to make their websites more responsive and reduce the amount of bandwidth they use. CDNs also provide a way for companies to ensure that their website is always available and deliver equivalent page loading times, no matter where an end user is located by connecting them to their closest content delivery server with the mirrored content. These networks also support load balancing, which ensures that the workload is spread evenly across all the servers in the CDN (Cloudflare, 2021).

CDNs have been around for decades, and they have been used by companies like Google, Facebook, and others, for years but are now being rapidly adopted by smaller organisations and individuals to host their website and application content, “By 2026, the CDN industry is expected to reach \$49.61 billion. That's a Compound Annual Growth Rate (CAGR) of 27.30%” (Todorov, 2022)

It is for this reason that many websites which would otherwise not be associated with Big Tech companies are now indirect subsidiaries in their delivery networks, as they continue to occupy more digital space. When running the lab in Scenario A, it will become obvious if a website relies on Big Tech to deliver their content, rather than their own website, when the firewall blocks the requests – though the HTML content will largely remain accessible, which is most important to the user.



**Figure 1: Typical Web Page Structure**

A webpage is made up of HTML, CSS, and JS. HTML provides the content and structure of the page. CSS provides a layout for the page. JS provides interactive features like animations or interactions with webpages.

Figure 1 shows the typical content that is usually provided to the client when accessing a web page. A majority of larger content CSS, JS, and media (Videos, Photos, File Downloads, etc) are usually offloaded to CDN services to reduce the load on web servers.

### **3.3. PRACTICAL SCENARIOS**

This section will explore in more detail the methodology and technical explanation of the two practical scenarios that will be set up, including the components and configurations.

#### **3.4. SCENARIO A – TOTAL DISCONNECTION**

Using publicised address ranges and entire TLD DNS blocks, access to all Big Tech-owned servers and addresses will be blocked by the firewall from accessing the Local Area Network. This will create a complete and total disconnection scenario to Big Tech-owned servers, whilst still maintaining access to the internet.

#### **3.5. SCENARIO B – SELECTIVE DISCONNECTION**

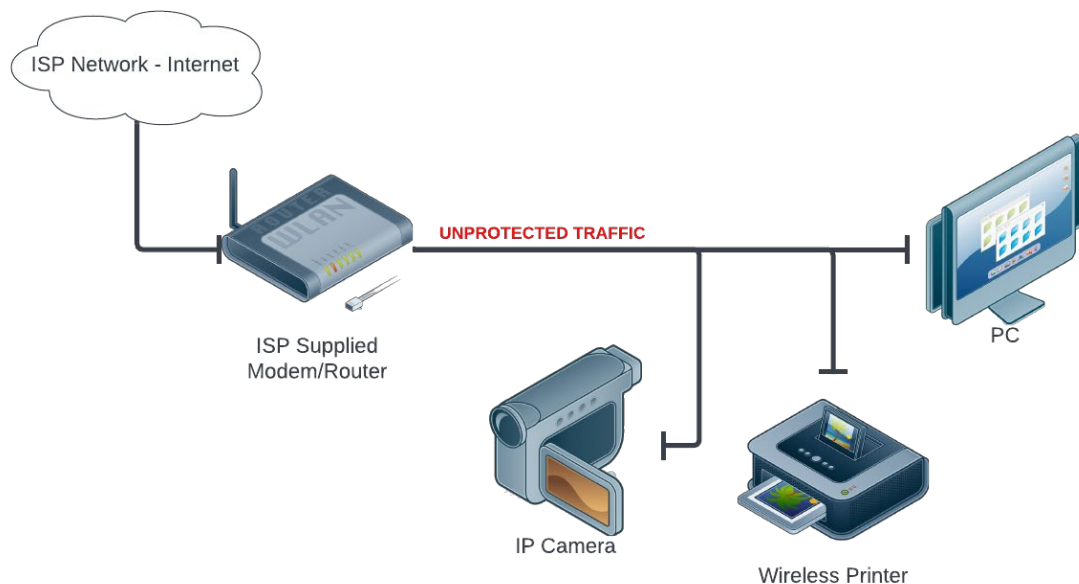
Selective disconnection will involve blocking only known subdomain lists that deliver additional unwanted and potentially hostile content to the client which is not required for the user to operate

the websites or services for their intended purpose (such as tracking, analytics, web advertisements, unneeded CDN content, etc).

This method will not be completely bulletproof in terms of filtering as the block lists that will be used are maintained by third-party sources and the frequency at which they are updated will not always be fast enough to cope with new additions to the Big Tech systems, DNS records and networks due to their vast size.

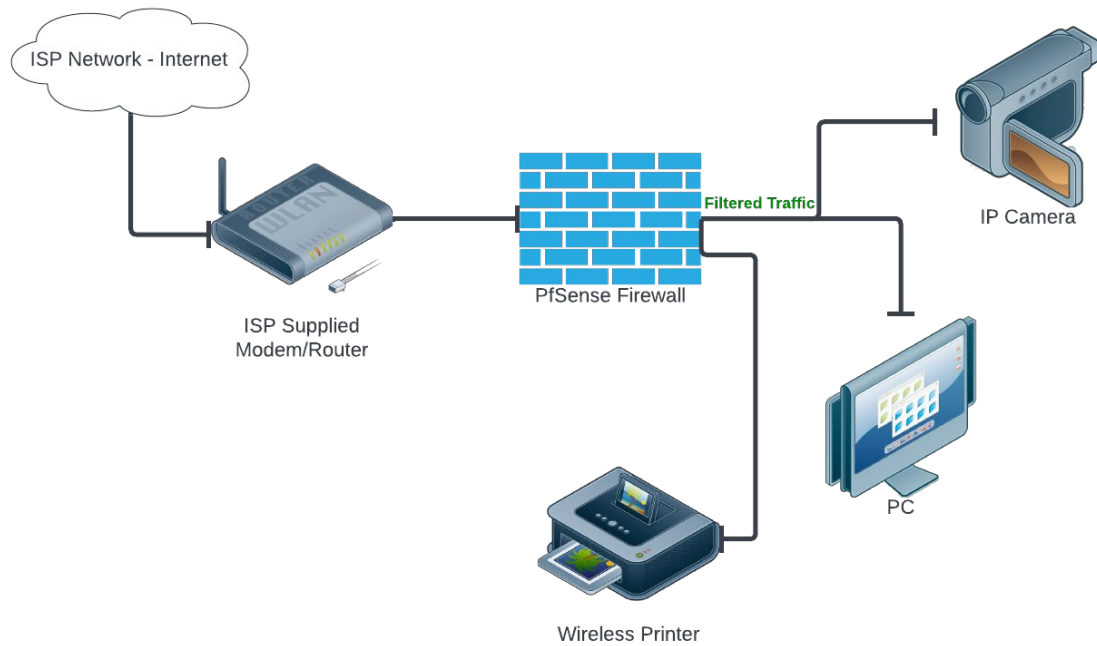
Both methods will require the use of the PfSense firewall rather than the typical consumer network that just uses the supplied router from the Internet Service provider. Pfsense is a FreeBSD-based firewall distribution that can be installed on a PC, firewall appliance or virtual machine. It has been designed to be easy to use and provides a robust set of features, including support for IPv6, OpenVPN, pfSense packages, and more (Kear, 2011).

### 3.6. FIREWALL APPLIANCE EXPLANATION



**Figure 2: Example Standard Unprotected Consumer Network [Logical Representation]**

Figure 2 shows an example of a standard unprotected consumer network in its most basic form of logical representation. A basic LAN consisting of a PC, IP Camera, and Wireless Printer. These devices are connected to the ISP Supplied Modem/Router, which does not have any sort of filtering rules and the consumer has little to no access in filtering the traffic that comes into their LAN through the router, represented as “Unprotected Traffic”. There are also a range of additional vulnerabilities that are caused by using the ISP supplied router solely to manage your network with, such as wireless vulnerabilities and exposure to more exploits (Terekhov, 2016).



**Figure 3: Example PfSense Filtered Traffic Network [Logical Representation]**

Figure 3 shows an example of a network protected by a PfSense firewall, whereby the traffic coming from the gateway (ISP Supplied Modem/Router) must pass through the firewall appliance before reaching the internal Local Area Network. Both Scenarios A and B will require firewall filtering rules. Filtered traffic as labelled on the diagram does not necessarily mean safe, it is an indication that the firewall is applying filtering rules to the traffic passing in and out of the network.

### **3.7. USE CASE APPLICATIONS**

By aligning the project with real world use case scenarios from different kinds of people of all age groups and occupations, it will offer a true representation of the level of disengagement that these people would have to endure to avoid using Big Tech monopoly services in their daily lives and will gauge how ingrained these services are into daily routines.

To set out the use case scenarios, a series of interviews and questionnaires have been used to collect qualitative data.

## 4. PRELIMINARY RESEARCH RESULTS

### 4.1. USER CLASSES

A series of interviews were conducted to find out the consequences of Big Tech disconnection on a range of user classes, after asking what Big Tech services each person uses and why. Based on this I then ranked each user on the level of consequences not using/having access to Big Tech services would have on them from Negligible to Detrimental.

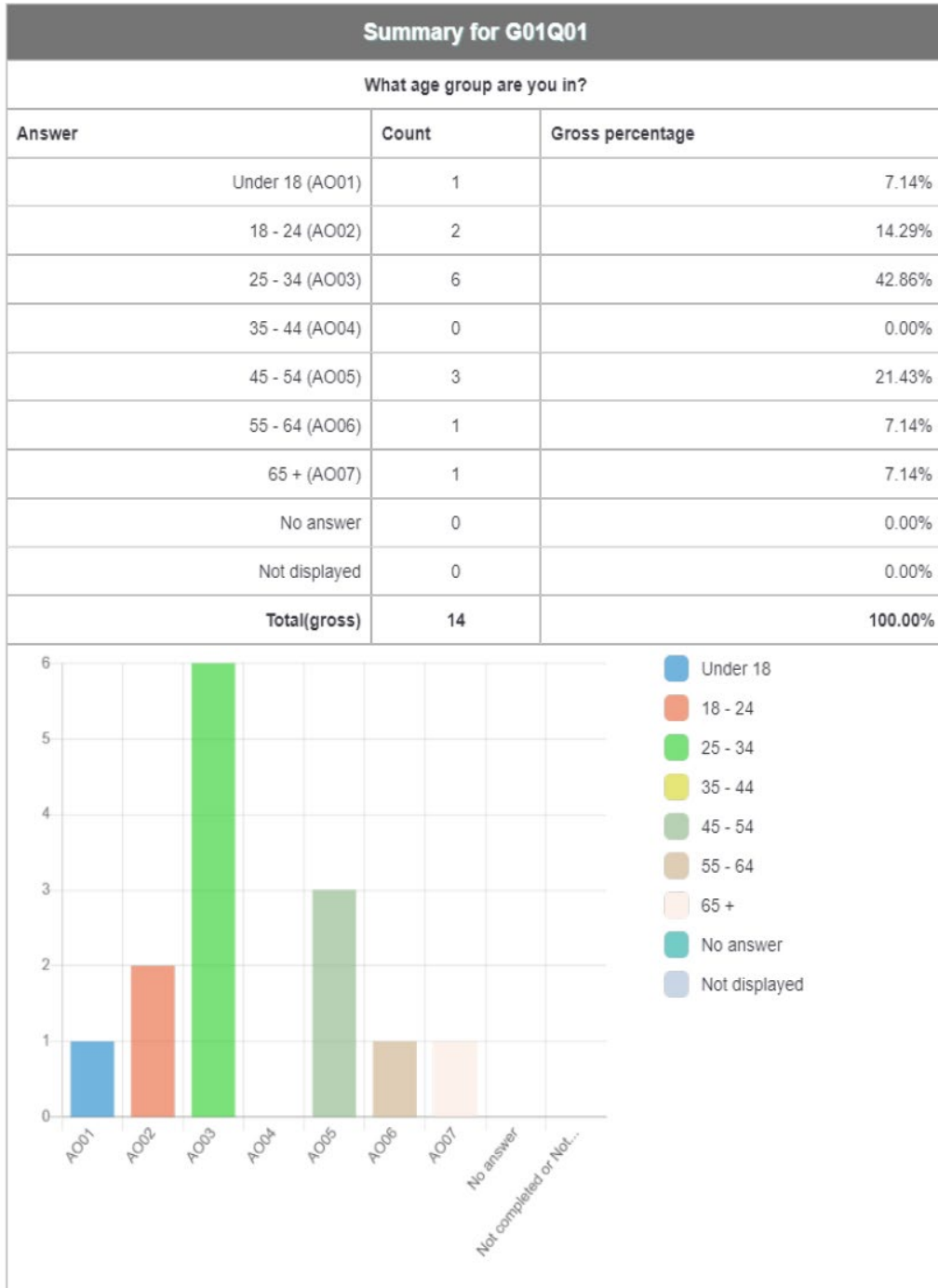
Name/Job Title	Services Used	Purpose & Why	Disconnection Consequences
Ed / Student	Microsoft Office / Outlook	Forced to use it because of University policies. Must use it to communicate with tutors and access educational services paid for.	Severe
Gary / Self-employed Mechanic	Google Mail	Gary is not comfortable with using his own mail server and knows that Google is a “well-known & trusted” email provider and says it doesn’t cost him anything, used for communicating with clients.	Minor
Ken / Landscape Gardener	Google Mail	Communicate with clients daily, “easy and free to use”. Was the first result when searching for “best free email” in Google.	Minor
Mike / Project Engineer	Microsoft Azure / Office / 365	Business relies on Microsoft to function. Sells Microsoft products to businesses to move their assets to Microsoft cloud services.	Detrimental
Joan / Retired Grandma	Apple Face Time	To communicate with Grandchildren alongside usual phone calls	Negligible
Samantha / NHS Employee	Microsoft Outlook & Teams	Used to communicate with her employees and have meetings as she works remotely. Due to NHS policy, no other applications can be used.	Detrimental
Stacy / Senior Solutions Engineer	Microsoft Teams & Outlook	Forced to use these applications due to company policy on data privacy. Meetings cannot be held via any other application, so use is required to keep job as the position is remote.	Detrimental
Stetson / DevOPS Engineer	Apple Products & Equipment / Microsoft Outlook & Teams	Supplied an iMac from employer, must use this to access applications only designed to run on Mac.	Detrimental
Yvonne / Mother	Google Mail	Has used Google Mail for years, always found it easy to use and is free of charge.	Minor

Figure 4: Big Tech Use Cases Table

Of those interviewed, 8/9 agreed that they are dependent in some way on Big Tech companies for their daily lives, whether that is for work or social purposes and all of them would be at least inconvenienced to a degree by the loss of service.

## 4.2. SURVEY

An anonymous preliminary survey was sent out to gain a wider view of Big Tech dependence. To ensure the survey results were balanced, 2 initial questions were asked to each participant – their age range and occupation. This helped to ensure that the results were not in reflection of a specific age group and occupation, for example, all 18 – 24-year-olds who are cyber security engineers.



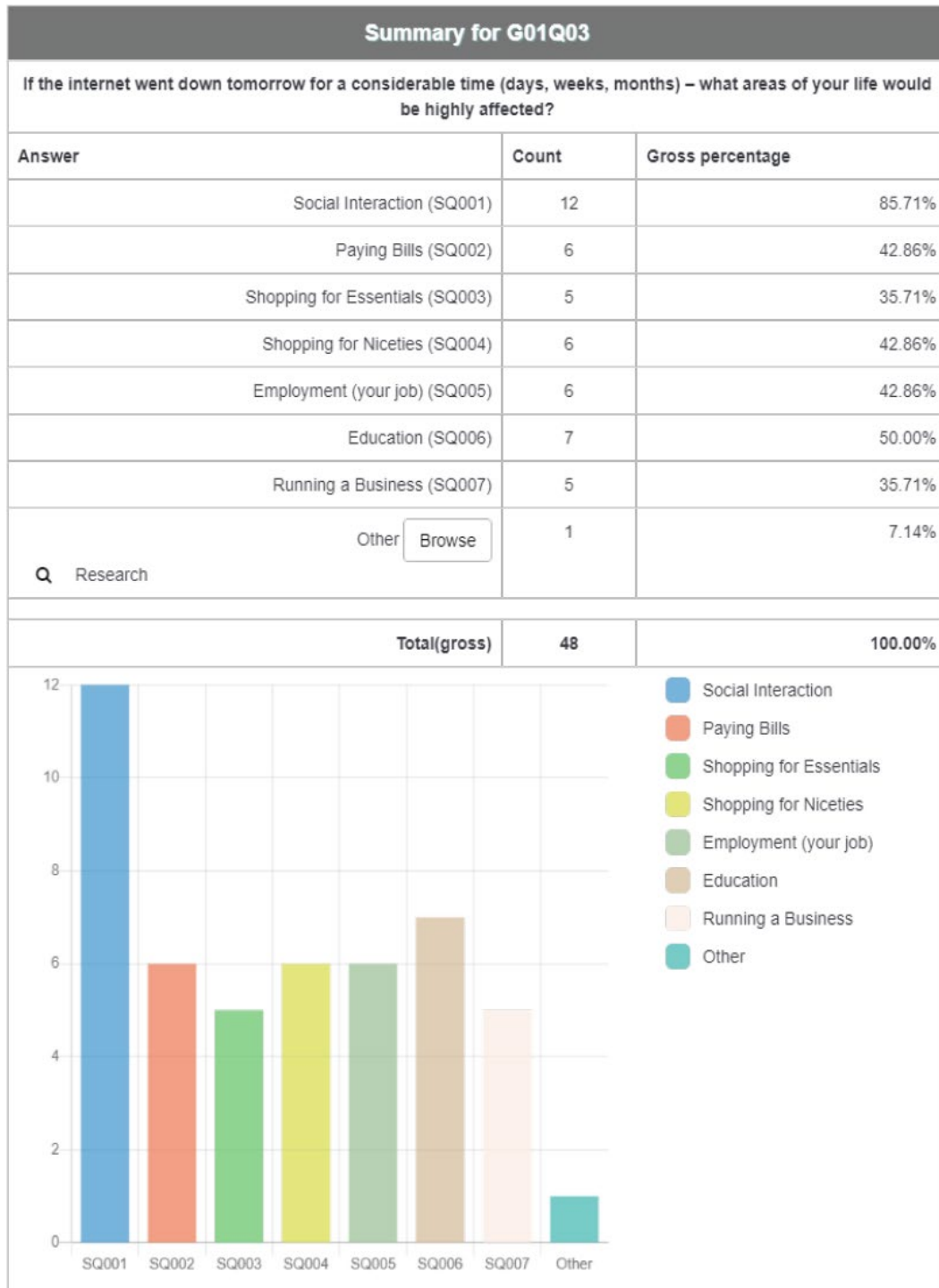
**Figure 5: Preliminary Survey Q01**

The results showed that there was a good balance of participants from all age groups (except 35 – 44) and occupations.

Summary for G01Q02		
What is your main occupation?		
Answer	Count	Gross percentage
<ul style="list-style-type: none"> <li>Q Postgraduate Student</li> <li>Q scientist</li> <li>Q Mother</li> <li>Q Student</li> <li>Q Full-stack Developer</li> <li>Q Mother</li> <li>Q Student</li> <li>Q School Student</li> <li>Q Software Engineer</li> <li>Q Builder</li> <li>Q IT Project Engineer</li> <li>Q NHS Occupational Therapist</li> <li>Q Mechanic</li> <li>Q Retired</li> </ul>	Answer <input type="button" value="Browse"/>	14 100.00%

**Figure 6: Preliminary Survey Q02**

The second question queried the occupation as mentioned above, from the individual results, there is an even spread of people taking part in the survey.

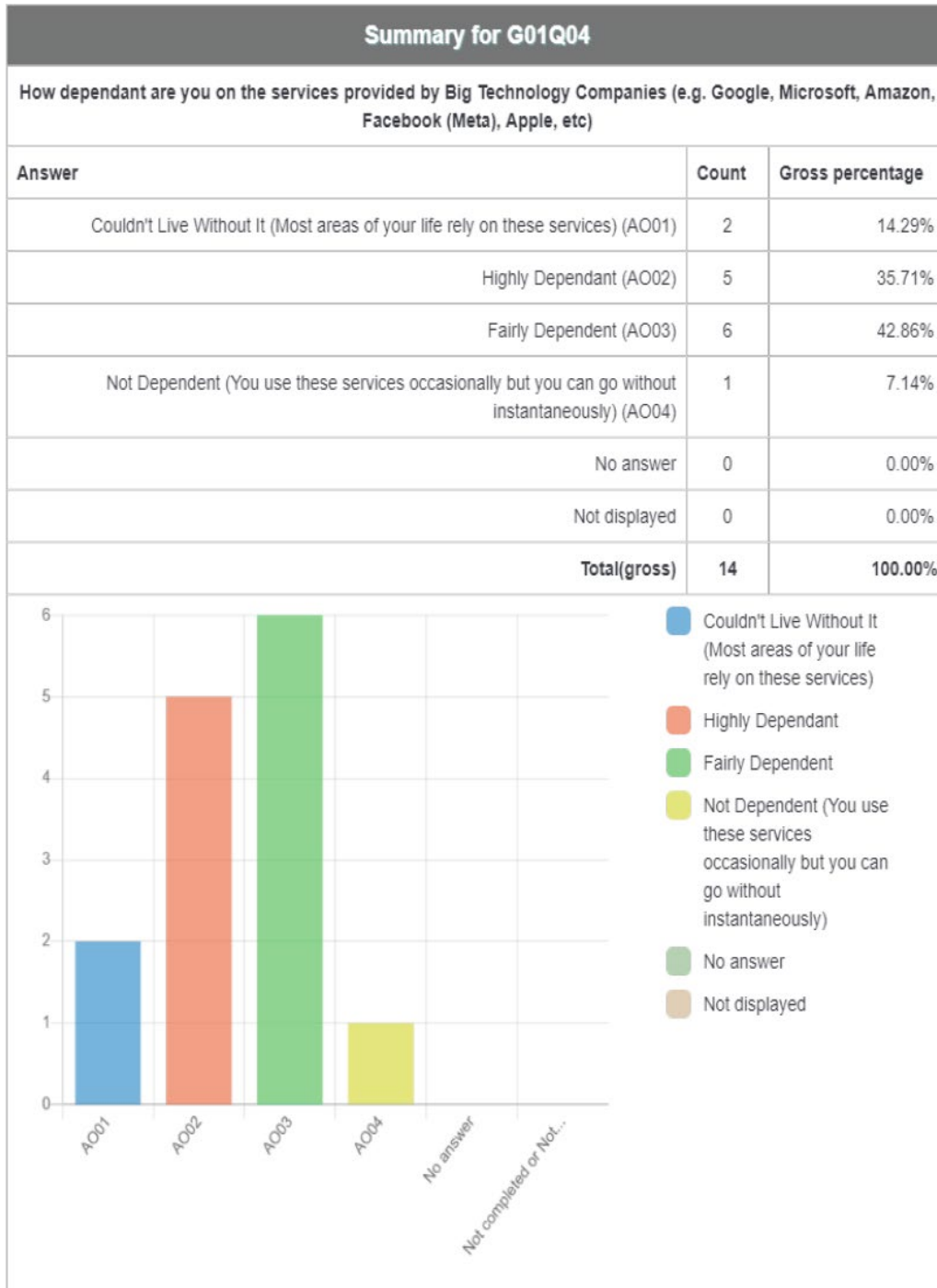


**Figure 7: Preliminary Survey Q03**

Over 85% of participants said that their social interaction would immediately be affected if they were not able to use the internet, followed by education (50%), paying bills, shopping for niceties and employment (42.86%), shopping for essentials and running a business (35.71%), and finally, one participant submitted “Research” as an “Other” option (7.14%).

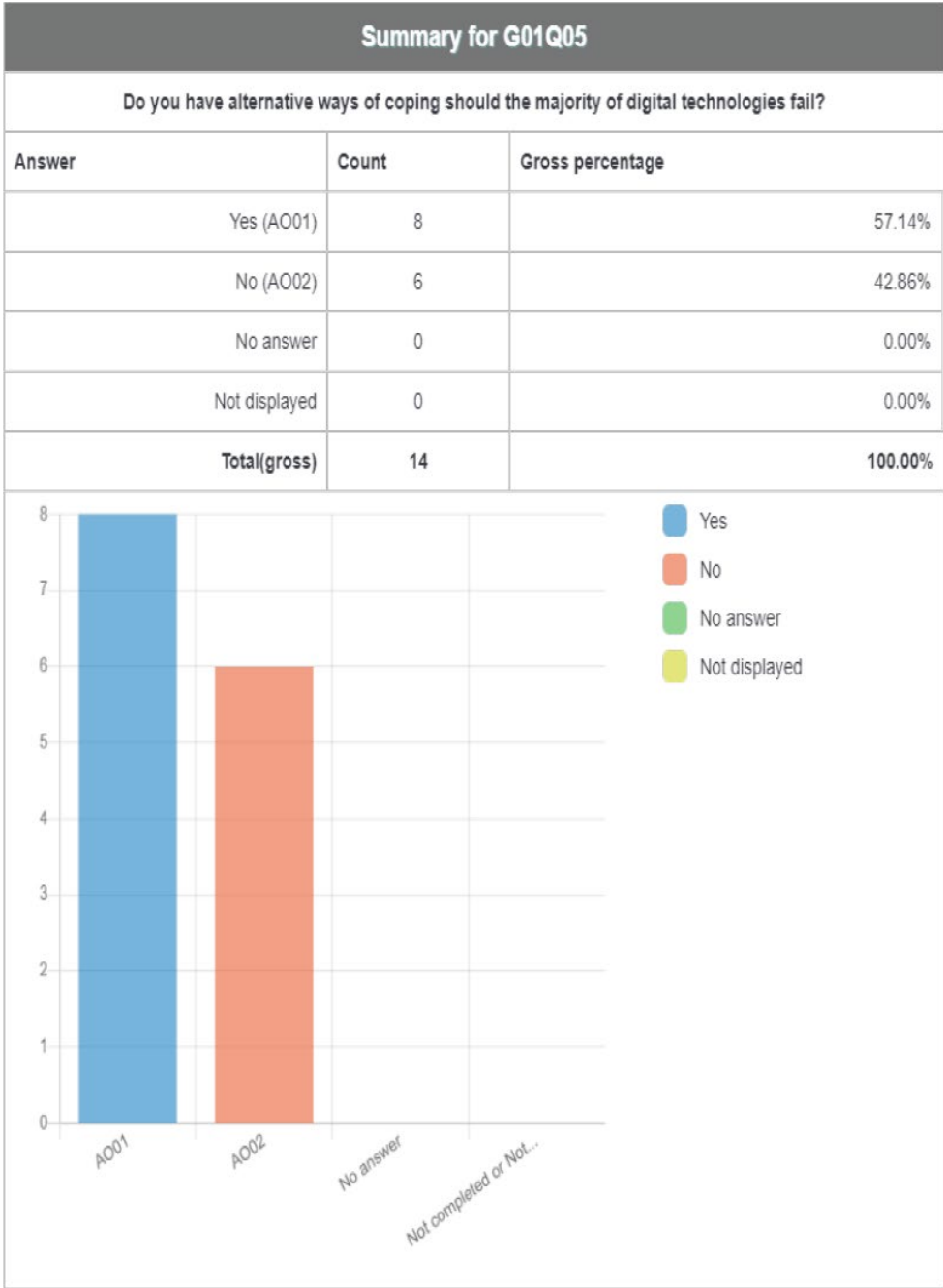
Interestingly, shopping for essentials is one of the least ticked options – whilst essentials can be bought online via online shopping methods, the price is usually elevated, and it is common knowledge that there are shops close enough to residential areas to buy essential goods.





**Figure 8: Preliminary Survey Q04**

92.86% (13/14) of the participants are dependent on Big Tech services in some form, whilst only 1 participant said they are not dependent. 14.29% said they could not live without these services, 35.71% said they were highly dependent on the services, followed by 42.86% being fairly dependent.



**Figure 9: Preliminary Survey Q05**

When asked the question “Do you have alternative ways of coping should the majority of digital technologies fail?”, only 57.14% of people said that they do (yes). 42.86% of people said they had no alternative ways of coping without digital technology in order to carry out their usual activities.

## Summary for G01Q06




If answered yes above, what coping mechanisms/backup plans do you have in place?

Answer	Count	Gross percentage
<p style="text-align: right;">Answer <input type="button" value="Browse"/></p> <ul style="list-style-type: none"> <li>Q Coded paper telephone and address book for friends and family as well as paper copies of banking information.</li> <li>Q Paper fallback methods</li> <li>Q Paper phonebook</li> <li>Q I have other educations I can put to use as a job. Most of my friends live locally so visiting won't be much of a problem.</li> <li>Q Cash, food and water, contact details and transport, survival manual offline. Medicines.</li> <li>Q Social - see friends in person. Know where they live.</li> <li>Q Go back to the old ways of holding records and billing customers. Just more time consuming.</li> <li>Q Do not particularly use the services anyway. I will call my grandchildren instead of face time. I have a telephone book and know where all my friends live.</li> </ul>	8	57.14%
No answer	6	42.86%
Not displayed	0	0.00%
<b>Total(gross)</b>	<b>14</b>	<b>100.00%</b>

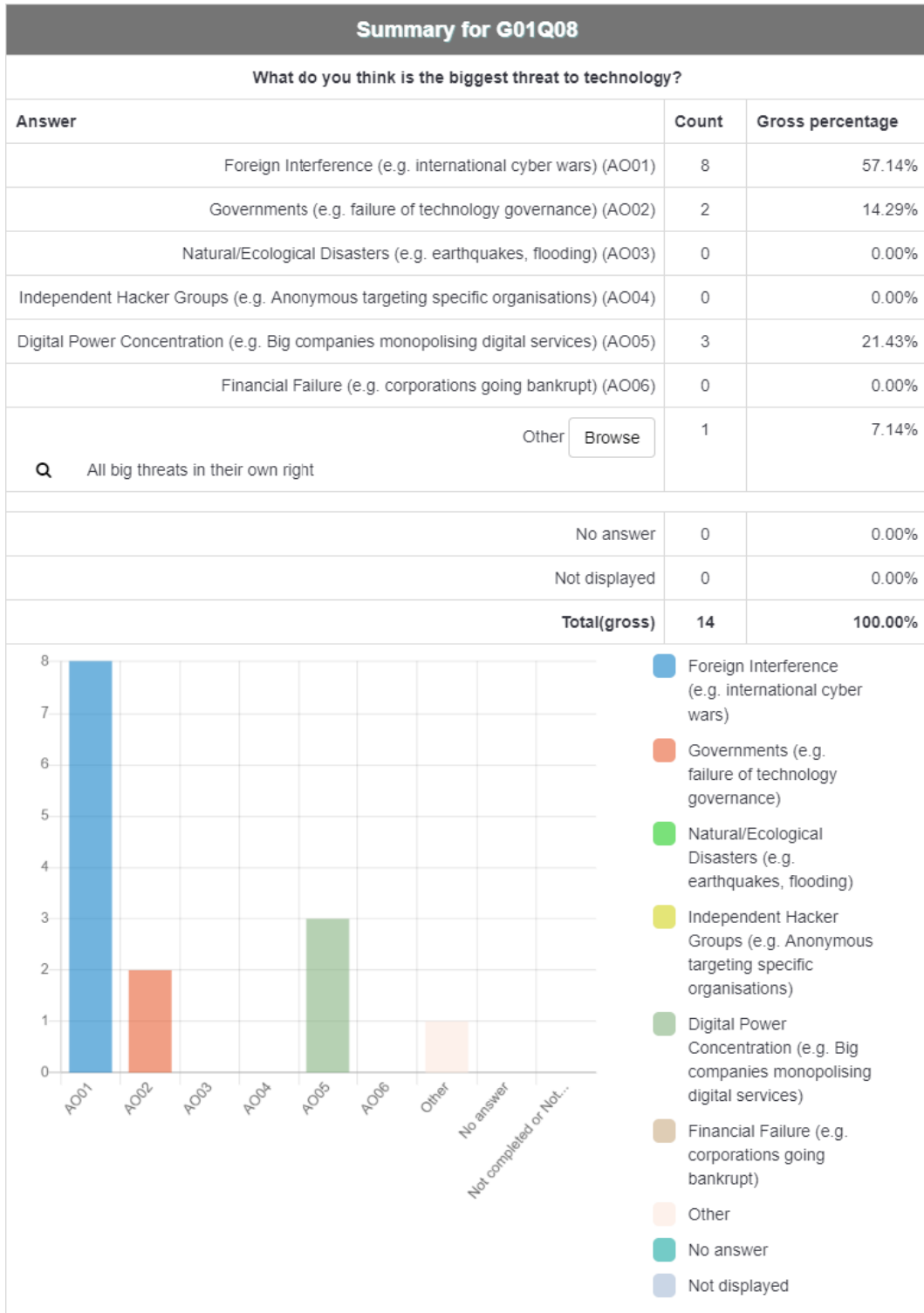
**Figure 10: Preliminary Survey Q06**

Most people who said they have backup mechanisms have mentioned the use of paper methods for phone numbers and home addresses as well as being aware of the geographical location of friends and where they live.

Summary for G01Q07 			
Who would/could you turn to in order to help manage technological resilience?			
Answer		Count	Gross percentage
	Answer <input type="button" value="Browse"/>	14	100.00%
Q	Myself		
Q	Personal social network of technical people		
Q	Son (Cyber Security Engineer)		
Q	Idk		
Q	My friend		
Q	Trained professionals		
Q	Build my own private cloud to store my data, and for emails.		
Q	Brother		
Q	Probably no one -- I need technology/connectedness to perform my job		
Q	don't know		
Q	Probably myself		
Q	Friends that work in IT		
Q	Not sure, myself?		
Q	Me		
	No answer	0	0.00%
	Not displayed	0	0.00%
	<b>Total(gross)</b>	<b>14</b>	<b>100.00%</b>

**Figure 11: Preliminary Survey Q07**

Most people that were asked who they could turn to in order to manage technological resilience said that they would use a close friend or family member, if not themselves.



**Figure 12: Preliminary Survey Q08**

The most chosen option from the single choice list for biggest threat to technology was foreign interference at 57.14%, followed by digital power concentration (21.43%) and finally Governments at 14.29%. The spike in Foreign Interference being a chosen option could be due to the current ongoing War in Ukraine making news headlines (Seibt, 2022).

## 5. PRACTICAL PROJECTS

Both two practical projects undertaken were created with the same goal – to increase awareness surrounding the dependency of Big Tech products and services. This section will explore in entirety the creation and testing process of two practical projects. The first is using a network firewall to block all devices on a LAN from being accessed by Big Tech owned IP Address ranges.

The second project is a website, “isitbig.tech”, which allows anyone to check a public URL (webpage) for dependency on Big Tech services, such as their CDNs, tracking, advertisement services, etc. This tool can be used to analyse potential websites by both

### 5.1. PFSense LAYER 3/4 BLOCKING

This project will involve interception of traffic both into and out of a isolated LAN, creating a protective atmosphere for all devices inside the network from transmitting or receiving any data from Big Tech owned IP Addresses specified within their ASNs. In turn, this will create a first-hand measurable experience for disconnection of Big Tech services and proportionately, how much of the internet becomes inaccessible or dysfunctional for the participants, each with a different use case.

#### 5.1.1. BACKGROUND & PRE-SETUP

This section will offer some insight into the background of PfSense, and the process of setting up the project.

##### 5.1.1.1 Why PfSense?

PfSense is a well-known firewall/routing open-source software based on the FreeBSD operating system. The project began in 2004 as a fork of a different project named “m0n0wall”, and its initial release was in 2006 (Fields, 2016). The project is widely supported and has been for over 16 years. Its extensive support, longevity and open-source status protrudes as a reliable and resilient platform to base the project on.

##### 5.1.1.2 Acquiring Hardware

The PfSense software is made to run on any hardware that uses the x86 architecture. The only limitations were that the device required enough memory, processing power and enough RJ45 ethernet ports for the project to function. Usually, network firewalls and routers do not require a lot of compute power, especially with modern processors – though this project will be using more compute power, especially memory, for caching entire ASN blocks of CIDR IP address ranges and checking all packets in and out the LAN at network & transport layers, against the cached addresses both into and out of the network. This process will use more memory than most firewalling and decided on a mid-range Intel i3-7167U CPU paired with 8GB of DDR4 memory.

The below table shows the relevant hardware specifications of the device:

Hardware	Specifications
Processor	Core i3 7167U Processor, 2.80 GHz, 3 MB Cache, 2 Cores 4 Threads, Iris Plus Graphics 650
I/O	4 x USB 3.0, 1 x HDMI, 6 x RJ45 Gigabit LAN, 1 x RS232 COM, 1 x RJ45 COM, 1 x DC IN, 1 x Power Switch
RAM	1x DDR4 8GB DIMM
NIC	6 x INTEL-I210/I211 Gigabit RJ45 LAN

Table 1: PfSense Hardware Specifications

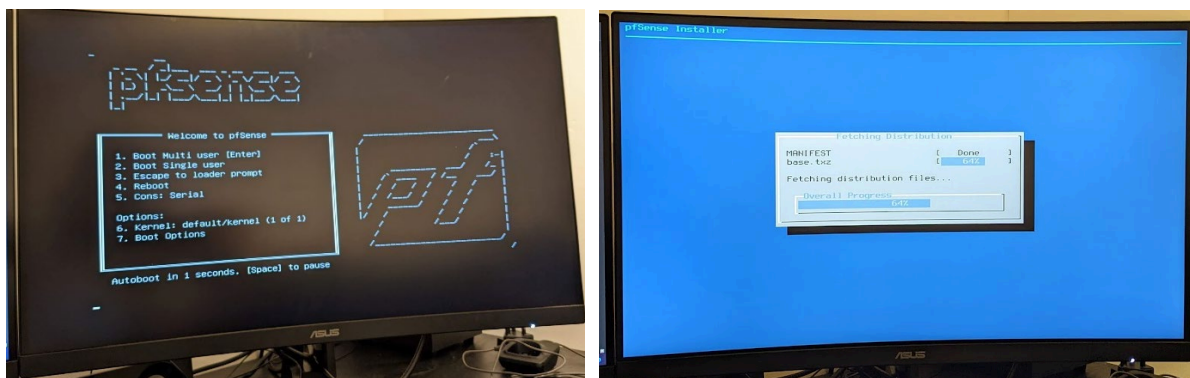


**Figure 13: pfSense Hardware**

Pictured above is an image of the physical firewall device. Port 0 (Red cable) is the WAN port; Port 1 is the LAN port.

### 5.1.1.3 Installation Process

The installation process was straightforward, the below screenshot displays the splash screen after booting from a USB flash drive created from the PfSense ISO file.



**Figure 14: PfSense Install Process**

The images below show a snapshot of the software installation. The installation time took around ~3 minutes in total. The process is mostly automated and very straightforward.

## 5.1.2. LOGICAL FUNCTIONALITY & VISUAL CONFIGURATION

This section will cover the logical plans and goals of the PfSense project.

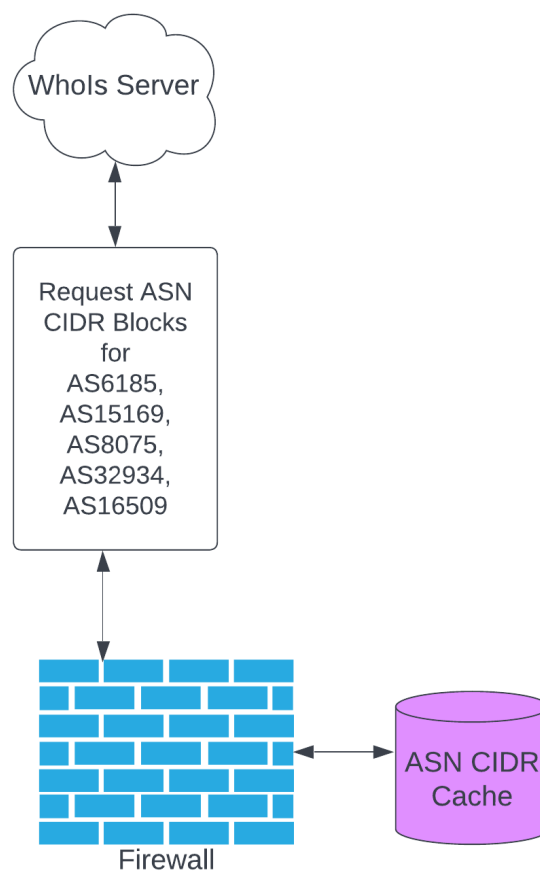
### 5.1.2.1 Firewall Functionality in Depth

The firewall will be making use of Autonomous System Numbers (ASNs) to effectively block all IP addresses, and therefore networks used and owned by the Big Tech corporations. An AS is another way to describe a large network and/or group of networks that all share the same routing policy. These policies are announced to the rest of the internet over the Border Gateway Protocol (BGP).

Each AS controls a specific set of IP addresses – hence why they are grouped together under one number. If two different IP addresses have the same AS number, they are operating under the same routing policy (Cloudflare, 2021). Therefore, it is very effective to block ASNs rather than blocks of IP

addresses. Nobody owns IP addresses, they are all leased from ICANN and therefore could be subject to change, “ICANN uses IANA, or the Internet Assigned Numbers Authority, to coordinate all IP addressing systems and autonomous system numbers. IANA functions as the system’s administrator that ensures every IP address is unique” (Račkauskas, 2021).

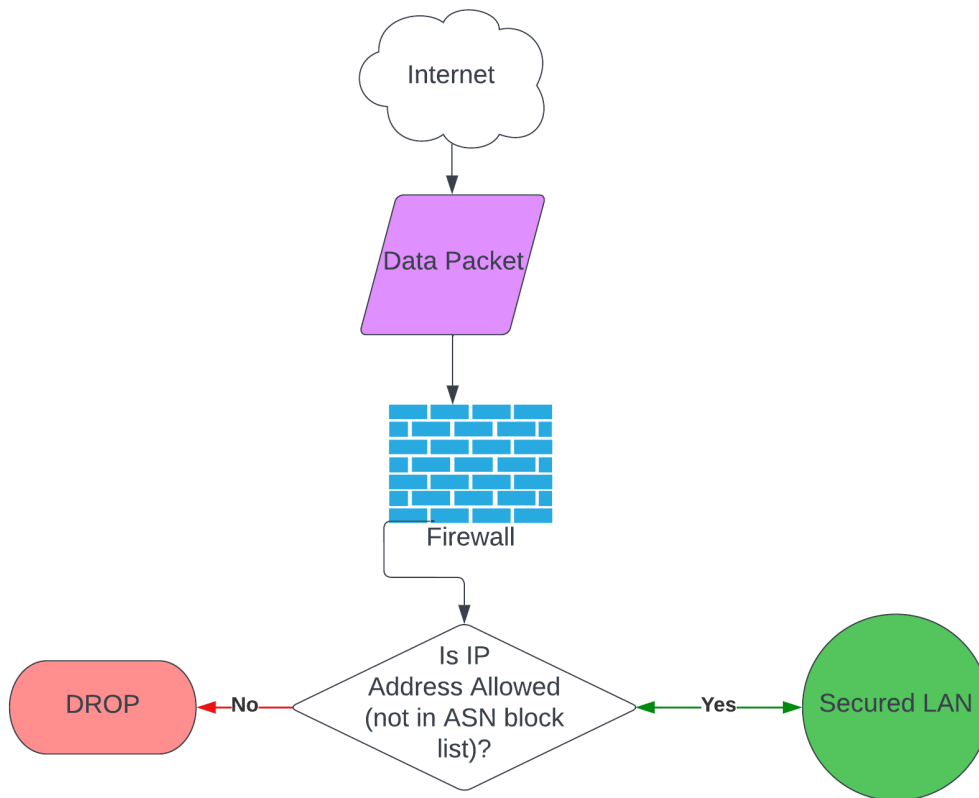
The firewall configuration makes use of a package called “pfBlocker-NG”. This package is what enables the mass grouping of IP addresses into a single alias/action (Netgate, 2022) – in this case, it is configured to “Deny Both” (Deny requests both inbound and outbound) to any IP address found within the ASN CIDR block list. PfSense can retrieve this information directly from running a WHOIS lookup. The firewall stores the CIDR IP address lists in its cache memory for quick local lookups and will run a WHOIS poll on an hourly basis to update the cache (if any new IP addresses or CIDR address ranges have been added/removed from the ASN). This process helps to ensure that the rules are always valid.



**Figure 15: PfSense WHOIS AS Request**

The above diagram is an example of how the initial and hourly AS request works, storing the retrieved data in the system cache (RAM) for immediate access. The AS Numbers listed above contain IP Address ranges owned by all Big Five companies.



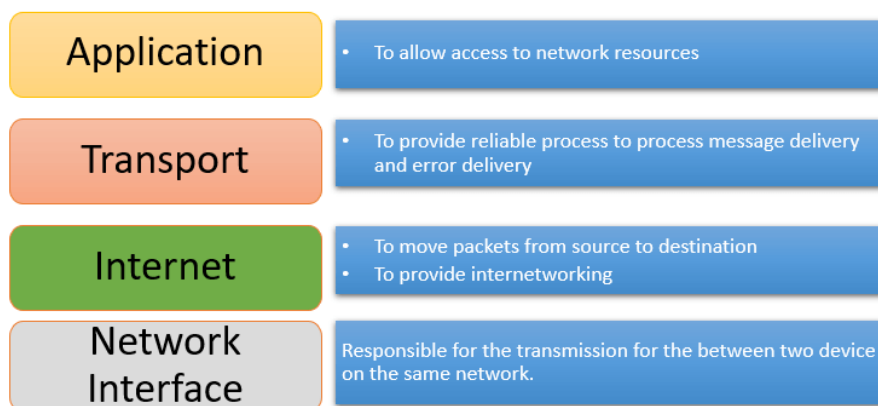


**Figure 16: PfSense Data Flow AS Block Check Process**

The above flowchart displays how the firewall deals with incoming requests with the firewall rules enabled – each packet header be inspected for its Source IP address (destination IP address from packets attempting to leave the secured LAN).

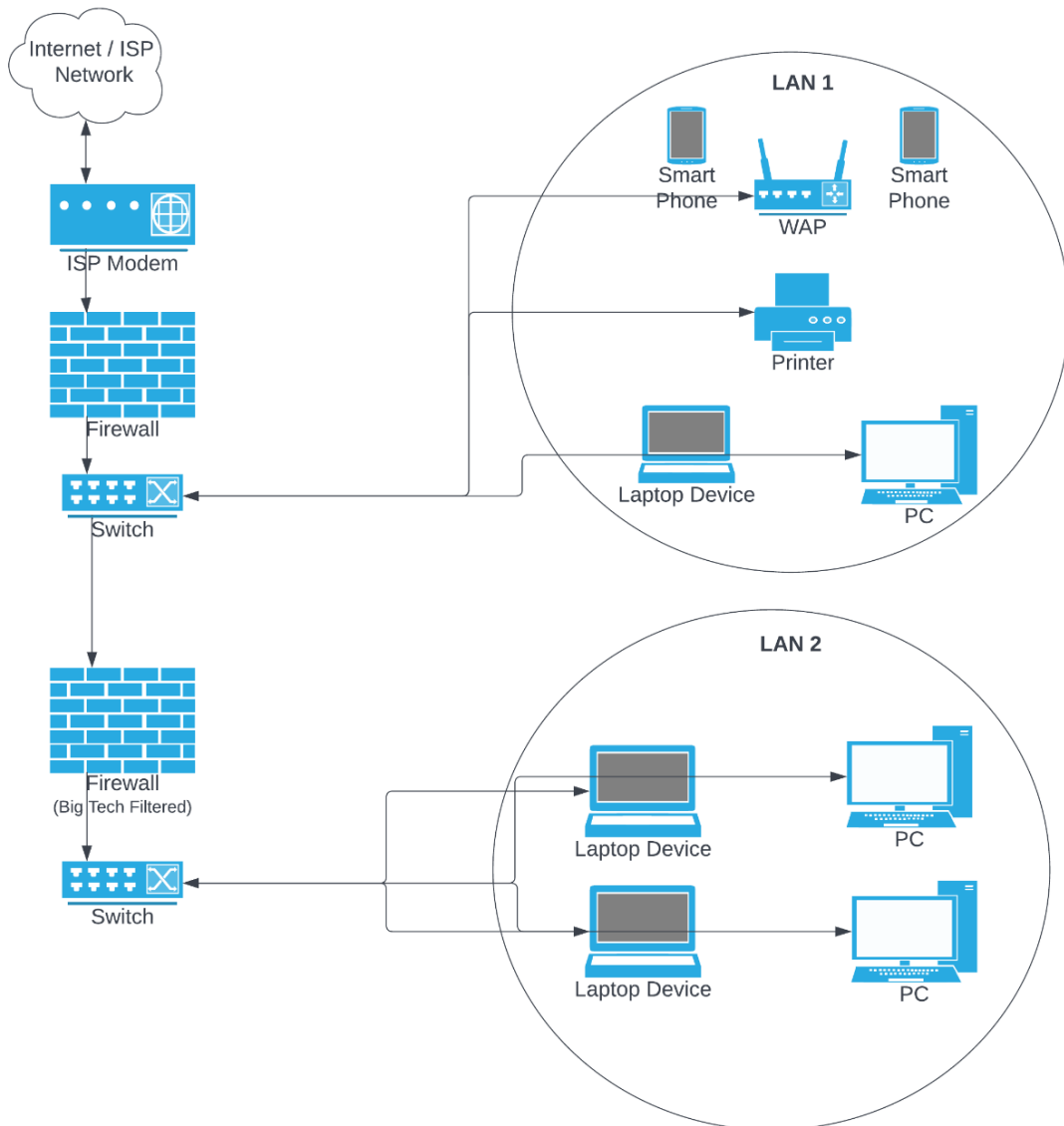
If the header of the packet is shown to have a source or destination address that is listed within the ASN Block list, the data will get dropped by the firewall and will not reach its destination.

This blocking takes place on the Network Layer of the OSI model – sometimes referred to as the internet layer on the TCP/IP Model (Williams, 2022).



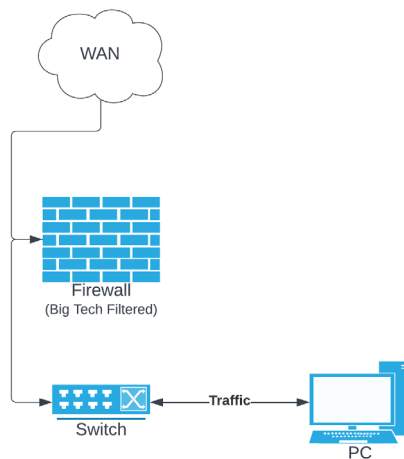
**Figure 17: Four Layers of TCP/IP Model (Williams, 2022)**

### 5.1.2.2 Network Topologies



**Figure 18: Wider Logical Network Topology**

The diagram shows the logical layout of the network upon which this project has been hosted on. I have ensured that the project activity is secured within its own LAN, and the only traffic passed between the firewall that serves and encapsulates LAN 2 is internet-bound traffic. The firewall serving LAN 2 has an operable DHCP server on a separate subnet (192.168.1.0/24). The reason this has been done is to protect the regular traffic from users in LAN 1 on a separate firewall as the gateway passes through the boarder gateway firewall before going out to the ISP network.



**Figure 19: Focused Network Topology**

The physical network area that will be explored within this project is a straightforward visualisation. The figure above shows an example of one of the devices on the new network (with the firewall included). Everything that leaves the firewall should be considered as potentially hostile.

### 5.1.3. CREATION OF RULES

Each IPv4 rule was added individually per company/AS Number that was being added to the blocking list. Each rule required an Alias Name, Description (human friendly), and list location settings. In the example below, the IPv4 list source/format is set to Whols, with the source being the AS Number, and the header as the company name (Apple). The list action is set to Deny Both – which as previously mentioned, will prevent traffic from all IP addresses within this list for inbound and outbound purposes.

IPv4 Settings	
LINKS <a href="#">Firewall Alias</a> <a href="#">Firewall Rules</a> <a href="#">Firewall Logs</a>	
Alias Name	<input type="text" value="ASN_Apple"/> ⓘ <small>Enter Alias Name (Example: Badguys) Do not include 'pfBlocker' or 'pfB_' in the Alias Name, it's done by package. International, special or space characters will be ignored in firewall alias names.</small>
List Description	<input type="text" value="AS Number Block for Apple (AS6185)"/>
List Settings	<span>ⓘ</span>
IPv4 Lists	<input type="text" value="Who"/> <input type="text" value="ON"/> <input type="text" value="AS6185"/> <input type="text" value="Apple"/> <small>Format State Source Header/Label</small>
Add	<input type="button" value="+ Add"/>
List Action	<input type="text" value="Deny Both"/> ⌵ <small>Default: Disabled ⓘ</small>
Update Frequency	<input type="text" value="Every Hour"/> ⌵ <small>Default: Never Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.</small>
Weekly (Day of Week)	<input type="text" value="Monday"/> ⌵ <small>Default: Monday Select the 'Weekly' ( Day of the Week ) to Update This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.</small>
Enable Logging	<input type="text" value="Enable"/> ⌵ <small>Default: Enable Select - Logging to Status: System Logs: FIREWALL ( Log ) This can be overridden by the 'Global Logging' Option in the General Tab.</small>
States Removal	<input type="text" value="Enable"/> ⌵ <small>With the 'Kill States' option (General Tab), you can disable States removal for this Alias.</small>

**Figure 20: ASN Firewall Rule Creation**

Firewall / pfBlockerNG / IPv4					
<a href="#">General</a> <a href="#">Update</a> <a href="#">Alerts</a> <a href="#">Reputation</a> <a href="#">IPv4</a> <a href="#">IPv6</a> <a href="#">DNSBL</a> <a href="#">GeoIP</a> <a href="#">Logs</a> <a href="#">Sync</a>					
Alias Name	Alias Description	Action	Frequency	Logging	
ASN_Apple	AS Number Block for Apple (AS6185)	Deny_Both	01hour	enabled	
ASN_Google	AS Number Block for Google (AS15169)	Deny_Both	01hour	enabled	
ASN_Microsoft	AS Number Block for Microsoft (AS8075)	Deny_Both	01hour	enabled	
ASN_Facebook	AS Number Block for Facebook (AS32934)	Deny_Both	01hour	enabled	
ASN_Amazon	AS Number Block for Amazon (AS16509)	Deny_Both	01hour	enabled	
					Add

Save

**Figure 21: Completed ASN Block List Rules (Big Tech)**

The above figure shows the completed list of ASN block rules on the firewall, all with the “Deny\_Both” action assigned, and 1 hour frequency updates from WHOIS services to ensure the cached IP addresses remain up to date.

```

=== [ IPv4 Process ] =====
[ Apple ]           Downloading update .. completed ..
[ Google ]         Downloading update [ 09/13/22 15:28:10 ] .. completed ..
[ Microsoft ]      Downloading update [ 09/13/22 15:28:11 ] .. completed ..
[ Facebook ]       Downloading update .. completed ..
[ Amazon ]         Downloading update [ 09/13/22 15:28:12 ] .. completed ..

=== [ Aliastables / Rules ] =====
Firewall rule changes found, applying Filter Reload

=== [ FINAL Processing ] =====

  [ Original IP count ] [ 25554 ]

=== [ Deny List IP Counts ] =====

25554 total
17290 /var/db/pfblockerng/deny/Amazon.txt
 7424 /var/db/pfblockerng/deny/Google.txt
  539 /var/db/pfblockerng/deny/Microsoft.txt
  220 /var/db/pfblockerng/deny/Facebook.txt
   81 /var/db/pfblockerng/deny/Apple.txt

```

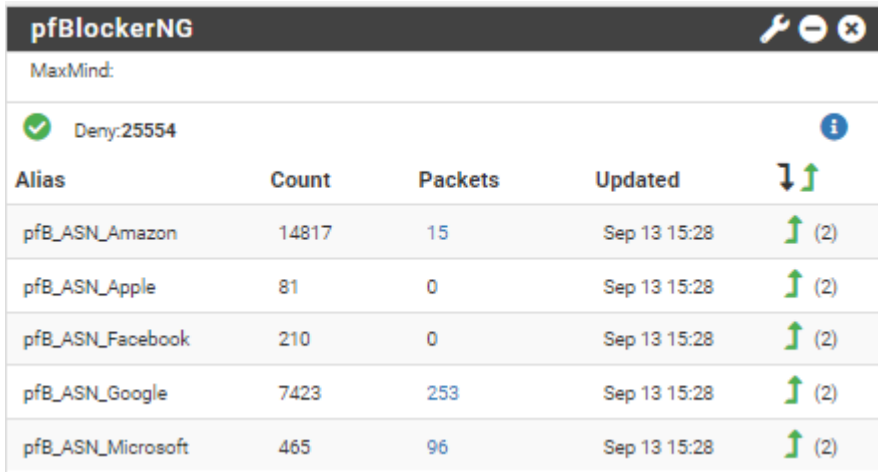
**Figure 22: PfBlocker-NG IPv4 Setup Process Logs**

The above shows that the IP lists have been successfully imported and identified by the rules configured – and cached into the local storage (/var/db/pfblockerng/deny/<list name>.txt).

25554 IP CIDR lists have been loaded in total, containing millions of addresses in total. This is a more efficient way (especially in binary) of processing the addresses rather than having to check a list for individual IP addresses, though it is expected the load will still be high on the processor.

## 5.1.4. TESTING

### 5.1.4.1 Initial Functionality Testing



Alias	Count	Packets	Updated	
pfB_ASN_Amazon	14817	15	Sep 13 15:28	↑ (2)
pfB_ASN_Apple	81	0	Sep 13 15:28	↑ (2)
pfB_ASN_Facebook	210	0	Sep 13 15:28	↑ (2)
pfB_ASN_Google	7423	253	Sep 13 15:28	↑ (2)
pfB_ASN_Microsoft	465	96	Sep 13 15:28	↑ (2)

Figure 23: pfBlockerNG ASN Packet Statistics

The initial test included connecting a lab machine to the LAN port of the firewall with a fresh Windows 11 installation. Within a few seconds of enabling the rules, the firewall began blocking packets from matched Amazon, Google, and Microsoft IP Addresses.

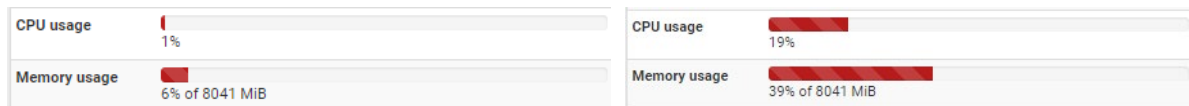


Figure 24: Hardware Usage (Idle vs Big Tech Traffic)

Initial memory and CPU usage was as expected, but the memory quickly began to fill up as more devices were added to the LAN.

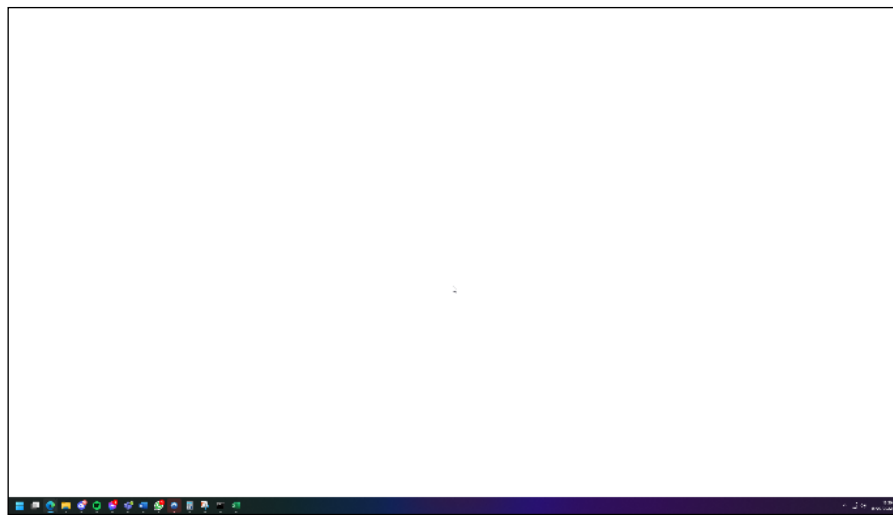


Figure 25: Windows 11 System Crash


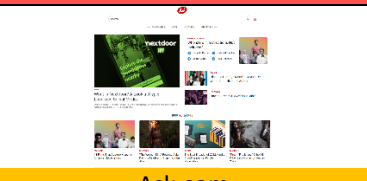
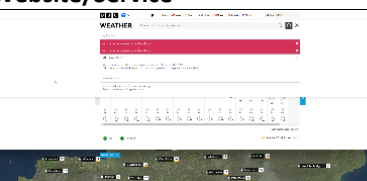
After a few minutes of the blocking rules being enabled, the Windows 11 browser, Microsoft Edge, completely crashed and became unresponsive. Shortly after, the GUI of the OS became unresponsive. Windows 11 has been criticised for its requirement for internet access to work properly, with the requirement for Microsoft accounts and internet access (Thomas, 2022) to install Windows, but system crashes have not been reported.

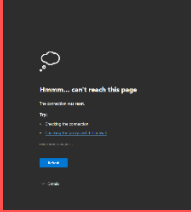
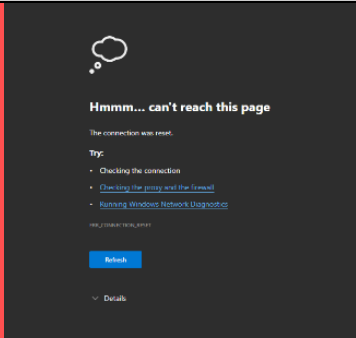
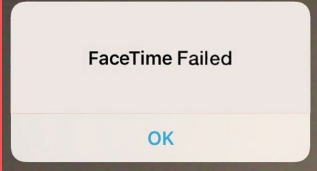
### 5.1.4.2 Key User Scenario Testing & Analysis (Results)

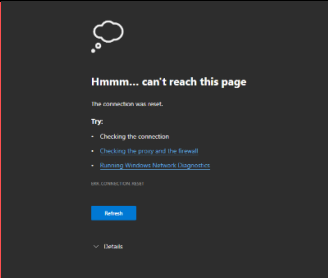
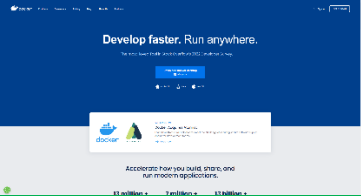
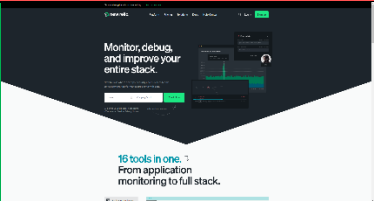
This section of the project testing measures user affectability. A selection of people tried to go about their usual internet activities on the LAN, without access to the Big Five’s systems and networks, to achieve their goals – from shopping to speaking to friends.

Key (Disconnection Type Scale)	Explanation
Detrimental	<i>Serious adverse effects on job or lifestyle, no option but to use.</i>
Major	<i>Serious affects with ability to engineer solutions</i>
Minor	<i>Feelings of disruption or disconnection, but not important.</i>
Negligible	<i>Causes minimal problems/inconvenience to user. Alternative options readily available.</i>

Table 2: Disconnection and Reliability Type Scale Key

Name/Job Title	Services/sites attempted to access	Disconnection Experiences & Comments		Disconnection Interruption
Gary / Self-employed Mechanic	MOT service portal, Ask.com	<b>Website/Service</b>  <b>MOT Service Portal</b> (www.check-mot.service.gov.uk) <b>Requires Google</b> Does not load.	<b>Comment</b> “A lot of our income is from MOT testing. I cannot do my job if I cannot access the portal.”	Detrimental – job and income are jeopardised and no alternative available.
		 <b>Ask.com</b> (https://ask.com) <b>Requires Google, Amazon</b> Loads, but not usable.	“Only search engine I could think of that isn’t ‘Big Tech’ but it doesn’t work. Only loads front page.”	
Ken / Landscape Gardener	BBC Weather, Gmail	<b>Website/Service</b>  <b>BBC Weather</b> (https://bbc.co.uk/weather) <b>Uses Amazon CDN for Postcode Search JS</b> Loads and usable if postcode area entered in URL (e.g., https://www.bbc.co.uk/weather/so15)	<b>Comment</b> “It works but I can’t enter a postcode otherwise it errors. I put the postcode in the URL and it renders.”	Minor – Ken stated he can move his email provider away from a Big Tech company and BBC weather still functional despite no postcode search – direct URL loads it.

		 <p>Google Mail (https://mail.google.com) <b>Requires Google</b> Does not load.</p>	<p>“Expected that to be the case, it is owned by Google. I could move email provider”</p>	
<b>Mike / Project Engineer</b>	Microsoft Office, Microsoft Azure	<p><b>Website/Service</b></p>  <p>Microsoft Azure &amp; Office (azure.microsoft.com &amp; office.com) <b>Requires Microsoft</b> Does not load.</p>	<p><b>Comment</b></p> <p>“As expected, these services will not work. Our entire business model is based on Microsoft as a Managed Service Provider – we sell their products to small businesses.”</p>	Detrimental – Mike’s entire company is built upon reselling Microsoft services and managing them for other businesses. They remove on-prem equipment in replacement for Microsoft Azure.
<b>Joan / Retired Grandma</b>	Apple FaceTime	<p><b>Website/Service</b></p>  <p>Apple FaceTime <b>Requires Apple</b> Does not work, “FaceTime Failed”.</p>	<p><b>Comment</b></p> <p>“This happens sometimes anyway; I have a phonebook of family numbers”</p>	Negligible – Facetime doesn’t work so she would just phone her family instead.
<b>Anon / NHS Employee</b>	NHS Website & Portals, Office 365	<p><b>Website/Service</b></p>  <p>auth.login.nhs.uk [108.138.217.110] <b>Requires Amazon</b> Does not load.</p>	<p><b>Comment</b></p> <p>“I didn’t know we use Amazon services for everything – that’s quite scary.”</p>	Detrimental – Anon cannot do their work without allowing Amazon to communicate with her network. NHS need Amazon Web Service’s network to load.
<b>Stacy / Senior Solutions Engineer</b>	DuckDuckGo	<p><b>Website/Service</b></p> <p>DuckDuckGo (duckduckgo.com)</p>	<p><b>Comment</b></p> <p>“I genuinely thought DuckDuckGo</p>	Detrimental – “Job is not operable without these

		<p><b>Requires Microsoft</b> Does not load</p>	would work – since when have they relied on Microsoft?”	apps and services. I learned that DuckDuckGo isn't as dependent as I thought too. They should change hosting companies”.
		<p>Jira Atlassian (jira.atlassian.com) <b>Requires RIPE</b> Does not load</p>		
		<p>DataDog (datadoghq.com) <b>Requires Amazon</b> Does not load</p>		
<b>Stetson / DevOps Engineer</b>	Travis CICD, Mongo DB, Atlassian/Jira, DataDog, Docker, Rapid7, Newrelic, Terraform Cloud	<p><b>Website/Service</b></p>	<b>Comment</b>	Detrimental – “I can't not use all these apps; I would never get a job in the DevOPS industry”
		 <p>Travis CICD (app.travis-ci.com) <b>Requires Google</b> Does not load</p>		
		<p>Mongo DB (www.mongodb.com) <b>Requires Amazon</b> Does not load</p>		
		 <p>Docker (docker.com) <b>Mostly Independent – Uses Google Tag Manager (not needed)</b> Fully Loads &amp; Apps Functional</p>		
		<p>Rapid7 (rapid7.com) <b>Requires Amazon</b> Does not load</p>		
		 <p>New relic (newrelic.com) <b>Mostly Independent – Uses</b></p>		



		<b>Cloudfront for Analytics</b> Fully Loads & Apps Functional		
		Terraform Cloud (app.terraform.io) <b>Requires Amazon</b> Does not load		
<b>Yvonne / Mother</b>	Spotify, YouTube, Google Mail	<b>Website/Service</b>	<b>Comment</b>	Major – “I was surprised by Spotify not working – I also had a hard time browsing other websites without a search engine!”
		Google Mail (mail.google.com) <b>Requires Google</b> Does not load		
		YouTube (youtube.com) <b>Requires Google</b> Does not load		
		Spotify (spotify.com) <b>Requires Google</b> Does not load	“I thought Spotify owned their own servers”	
<b>Arny / Property Maintenance</b>	RightMove, eBay	<b>Website/Service</b>	<b>Comment</b>	Negligible – “I’m glad that the two websites I use the most aren’t reliant on Big Tech companies – but I will need to kick the habit of typing the sites into Google!”
		RightMove (rightmove.co.uk) <b>Mostly Independent – Uses Google Tag Manager (not needed)</b> Fully loads & functional		
		Ebay (ebay.co.uk) <b>Independent</b> Fully loads & functional		

*Table 3: User Affectability – Disconnection and Reliability Experiment*

### 5.1.5. CONCLUDING PROJECT COMMENTS

This project was very eye-opening for the participants, and without having first-hand experience trying to navigate the surface web and popular sites minus the services offered by Big Tech, it’s difficult to understand how many websites and services they really do have control over.

Most of the participants asked whether the internet “was still online” until they were shown some independent websites loading successfully. The table above is only a handful of results, but the second part of the project should offer some awareness to accompany this experiment as to how vast this reliance has become and how feeble this makes cloud computing and therefore, the internet.

## 5.2. IS IT BIG TECH WEBSITE (ISITBIG.TECH)

This second project aims to accompany the PfSense disconnection project in terms of raising awareness of Big Tech dominance and how much we rely on these five companies to keep a huge portion of the internet running. This project aims to allow anyone to input a URL of an existing website on the internet, and will inspect the fully rendered webpage for any Big Tech external content

### 5.2.1 BACKGROUND & PRE-SETUP

This section will explore the technologies chosen and the dev environment used to deploy the web application.

#### 5.2.1.1 Puppeteer – the high-level Chromium API

Puppeteer is a Node library API for the Chromium browser. To analyse the webpages and sites that are inputted for Big Tech dependency, the site will need to be rendered in the same way as a normal user would've accessed it via their web browser – this library is one of the easiest ways to do this and therefore Node will be chosen as the backend for this project as it is highly supported with the correct dependencies.

#### 5.2.1.2 Web Server Configuration

To serve the content of the NodeJS server to the web, a few things needed to happen:

##### ❖ Configure an internal proxy to forward the content to external web ports

To serve the content to the external network and properly manage the traffic and handle the necessary certificates, an Nginx server is used. Below is a screenshot of the configuration file for the Nginx server.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    root /var/www/isitbigtech;
    server_name _;
    location / {
        proxy_pass http://127.0.0.1:3000;
    }
}
```

Figure 26: Nginx Proxy Basic Configuration (/etc/nginx/sites-enabled/default)

The above figure shows the basic configuration to serve HTTP clients and is using a basic “proxy\_pass” to pass anything from the locally hosted port 3000 to port 80, which is enabled on the firewall. This will enable all port 80 clients to view the NodeJS server.

##### ➤ Enable HTTPS & obtain an SSL certificate

Using the CertBot package on Ubuntu, a LetsEncrypt keychain pair was generated to provide the SSL certificate and ensure the connection between the client and server is end-to-end encrypted over port 443.

```

server {
    root /var/www/isitbigtech;
    server_name isitbig.tech; # managed by Certbot
    location / {
        proxy_pass http://127.0.0.1:3000;
    }
    listen [::]:443 ssl ipv6only=on; # managed by Certbot
    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/isitbig.tech/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/isitbig.tech/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}

server {
    if ($host = isitbig.tech) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    listen 80 ;
    listen [::]:80 ;
    server_name isitbig.tech;
    return 404; # managed by Certbot
}

```

Figure 27: Nginx Proxy SSL Certbot Configuration (/etc/nginx/sites-enabled/default)

Above is a screenshot of the config file for the HTTPS proxy pass connection, served via the Nginx server.

➤ **Ensure the NodeJS process stays alive**

By default, the NodeJS application only runs when a user executes the command to do so. PM2 is a process manager for NodeJS (PM2, 2022); this is what was used to ensure that the application always remained on. It can be installed via the Node Package Manager.

```

root@srv2:~# pm2 status

```

id	name	namespace	version	mode	pid	uptime	Ⓜ	status	cpu	mem	user	watching
0	isitbigtech	default	1.0.0	Fork	72494	47h	7	online	0%	111.4mb	nginx	disabled

```

[PM2][WARN] Current process list is not synchronized with saved list. App index differs. Type 'pm2 save' to synchronize.
root@srv2:~#

```

Figure 28: PM2 Status Output

Above is an output of the “pm2 status” command, which shows all the current NodeJS applications running as services under the PM2 manager. The above output indicates that the application is running correctly.

### 5.2.1.3 Development & Hosting Environment

Due to the nature of the application, it is essential that it is completely independent and operates effectively. The website is hosted on a Linux-based Dedicated Server in a German Datacentre, operating completely dependently.

To ensure changes were kept track of when developing the application, I used a GitHub repository to ensure workflow was optimised as much as possible throughout. Development was done locally and then the server pulled the changes from the GitHub repository when appropriate, therefore going via 2 stages of testing (locally and in production). The figure below shows the commits made to the repository (newest to oldest).

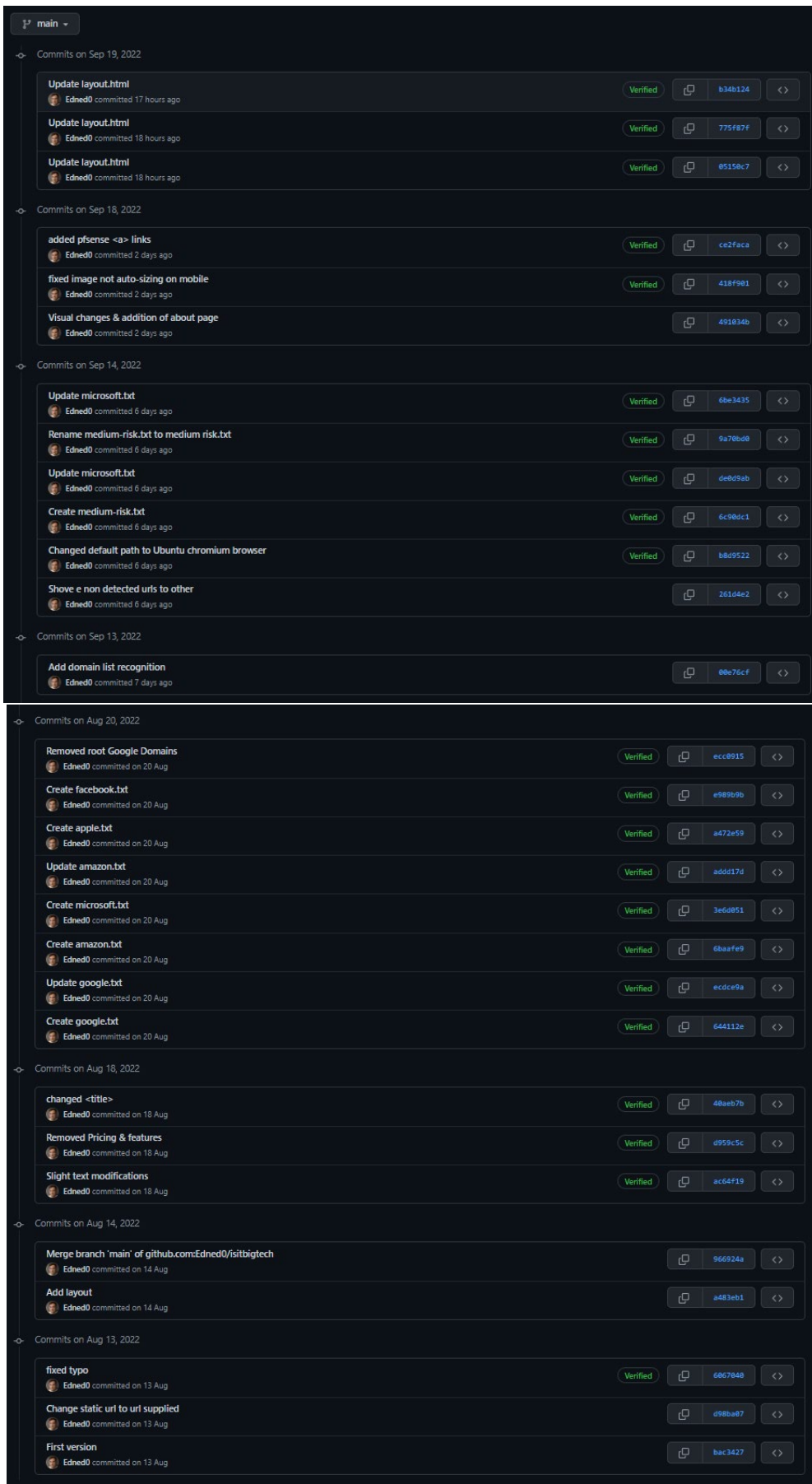


Figure 29: IsItBigTech Git Commits

## 5.2.2 LOGICAL FUNCATIONALITY

### 5.2.2.1 Logical Process Representation

The figure below describes the essential functionality of the application, the user will input their URL into the HTML form on the index page, the application will then pass this URL to the Puppeteer module, which then launches a chromium browser process using the URL. Once rendered, the URLs found in the webpage will be sent for processing – at this stage, the URLs are checked against the domain lists cached when the application starts. If a domain is found, it will be sorted under the tab for this domain. All remaining URLs are then shown under the “Other” tab on the front-end page, which is re-rendered when the application has finished processing the webpage for all links that are found.

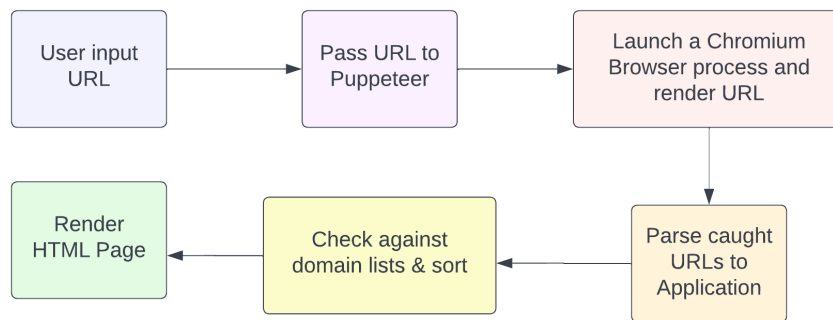


Figure 30: Website Logical Process Representation

### 4.2.1.1 File & Folder Structure

The figure below represents the file structure of the application, displaying all its component files and folders. All components in the “src” directory are loaded and/or rendered from index.js.

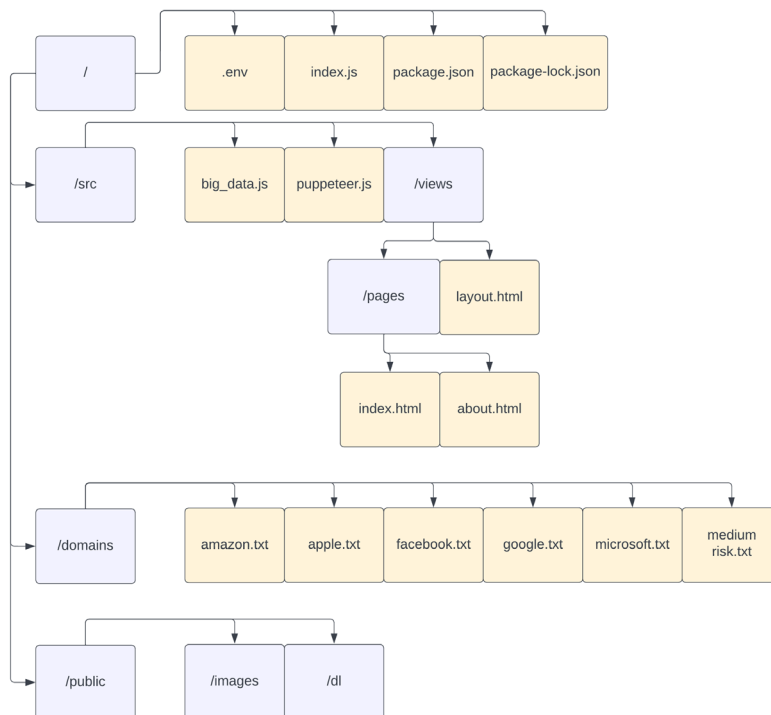


Figure 31: IsItBigTech Application File & Folder Structure

## 5.2.3 BRIEF ESSENTIAL CODE EXPLANATION

### 5.2.3.1 Index.js

```
1  require('dotenv').config()
2
3  const express = require('express');
4  const ejs = require('ejs').__express;
5  const expressLayouts = require('express-ejs-layouts');
6  const path = require('path');
7  const bigData = require('./src/big_data');
8  const puppeteer = require('./src/puppeteer');
9  const _ = require('lodash');
10
11 const app = express();
12 const port = 3000;
13
14 app.use(expressLayouts);
15 app.engine('html', ejs);
16 app.set('views', path.join(__dirname, 'src', 'views'));
17 app.set('layout', 'layout');
18 app.set('view engine', 'html');
19 app.use(express.json());
20 app.use('/images', express.static(__dirname + '/public/images'));
21 app.use('/dl', express.static(__dirname + '/public/dl'));
22
23 bigData.readUrls('./domains/');
24
25 app.get('/', (req, res) => {
26   res.render('pages/index');
27 });
28
29 app.get('/about', (req, res) => {
30   res.render('pages/about');
31 });
32
33 app.post('/check', async (req, res, next) => {
34   //TODO: Make sync
35   //TODO: Check url
36
37   const [links, screenshot] = await puppeteer.getHtmlAndScreenshot(req.body.url);
38   const urls = Object.assign({}, await bigData.filterBigData(links));
39
40   return res.json({
41     urls,
42     screenshot
43   });
44 });
45
46 app.listen(port, () => {
47   console.log(`IsItBigTech listening on port ${port}`);
48 })
```

Figure 32: IsItBigTech - index.js

The application launches from this file, it is the anchor that ties all the elements of the application together. Line 1 includes the '.env' configuration file. Lines 3 – 12 assign variables to modules, paths, and values to make calling them easier throughout the application. Lines 14 – 21 configure the express paths, and sets the view engine, etc. Line 23 tells the big\_data.js script to read the URLs from all the text files in the domains directory. Lines 25 – 31 set the render paths for the public view pages (index and about). Lines 33 – 44 returns the data back to the front end once processed. Lines 46 – 48 tells express to listen on the port specified in the variable at the top of the file (3000 in this case).

### 5.2.3.2 /src/big\_data.js

```
1  const regex = new RegExp(/(?:https?:\/\/)(?:www.)?[^?=\r\n|\|\/\\]+\.\w+\/igm);
2  const fs = require('fs');
3  const _ = require('lodash');
4
5  async function readUrls(dir)
6  {
7      global.domainCache = [];
8
9      fs.readdirSync(dir).forEach(file => {
10         if (!file.endsWith('.txt')) {
11             return
12         }
13
14         const company = file.slice(0, -4);
15         global.domainCache[company] = [];
16
17         const domains = fs.readFileSync(dir + file, 'utf8');
18         domains.split(/\r?\n/).forEach(line => {
19             if (line.length > 0) {
20                 global.domainCache[company].push(line);
21             }
22         });
23
24         console.log('Cached: ' + file);
25     });
26 }
27
28 async function filterBigData(data)
29 {
30     const cache = global.domainCache;
31     let urls = [];
32
33     data.forEach(html => {
34         const result = regex.exec(html);
35
36         if (result == null || result[0] == null) {
37             return;
38         }
39
40         urls.push(result[0]);
41     })
42
43     urls = urls
44         .sort()
45         .filter(function(item, pos, ary) {
46             return !pos || item != ary[pos - 1];
47         });
48
49     const caught = [];
50     const other = [];
51
52     urls.forEach(url => {
53         for (const [company, domains] of Object.entries(cache)) {
54             domains.forEach(domain => {
55                 if (url.includes(domain)) {
56                     if (!caught.hasOwnProperty(company)) {
57                         caught[company] = [];
58                     }
59
60                     caught[company].push(url);
61                 } else if (!other.includes(url)) {
62                     other.push(url);
63                 }
64             })
65         });
66     });
67
68     caught['other'] = other;
69
70     return caught;
71 }
72
73 module.exports = {
74     readUrls, filterBigData
75 }
```

Figure 33: IsItBigTech - /src/big\_data.js

Line 1 defines the Regexp expression used for locating URLs within the rendered webpages. Anything that matches this expression will be captured.

Lines 2-3 requires the import of fs (File System) and lodash modules.

Lines 5 – 26 (readUrls function) reads through all the files within the domains folder and caches them using the file name (assigned as company) and strips the txt file extension from this. This is done for every file in the directory, and a console log is running every time it completes caching a file’s URLs for Realtime use in the application.

Lines 28 – 71 (filterBigData function) uses the cached domains (assigned to a variable called cache) and uses a forEach loop to check each HTML element against the Regexp Expression previously set in the file. If any content is found in the webpage that matches the regex expression, it sorts and filters it against the cached Big Tech URLs, if it does not match any URLs set in the text files, the Regexp match (URL) will be put into the “Other” heading.

Lines 73 – 75 instructs Node to export the data from both functions above to the rest of the application files, to parse this back to the index view.

### 5.2.3.3 /src/puppeteer.js

```
1  const puppeteer = require('puppeteer-core');
2
3  async function getHtmlAndScreenshot(url)
4  {
5      const browser = await puppeteer.launch({executablePath: process.env.PUPPETEER_EXECUTABLE});
6      const page = await browser.newPage();
7      await page.goto(url, { waitUntil: 'networkidle0' });
8
9      const screenshot = await page.screenshot({ encoding: "base64" });
10     const data = await page.evaluate(
11         () => Array.from(document.querySelectorAll('*'))
12             .map(elem => elem.outerHTML)
13     );
14
15     browser.close();
16
17     return [data, screenshot];
18 }
19
20 module.exports = {
21     getHtmlAndScreenshot
22 }
```

Figure 34: IstBigTech - /src/puppeteer.js

The main purpose of this file is to grab the data to feed into the big\_data.js script above. When a URL is entered, Puppeteer will launch a new Chromium browser process, open a new page, take a screenshot of the loaded page (waits for networkidle0), and then grabs all outerHTML from the page. Once this is complete, the browser is closed, and the data is exported using module exports back to the rest of the application.



## 5.2.4 PUBLIC VIEWABLE PAGES

### 5.2.4.1 Index (Home)

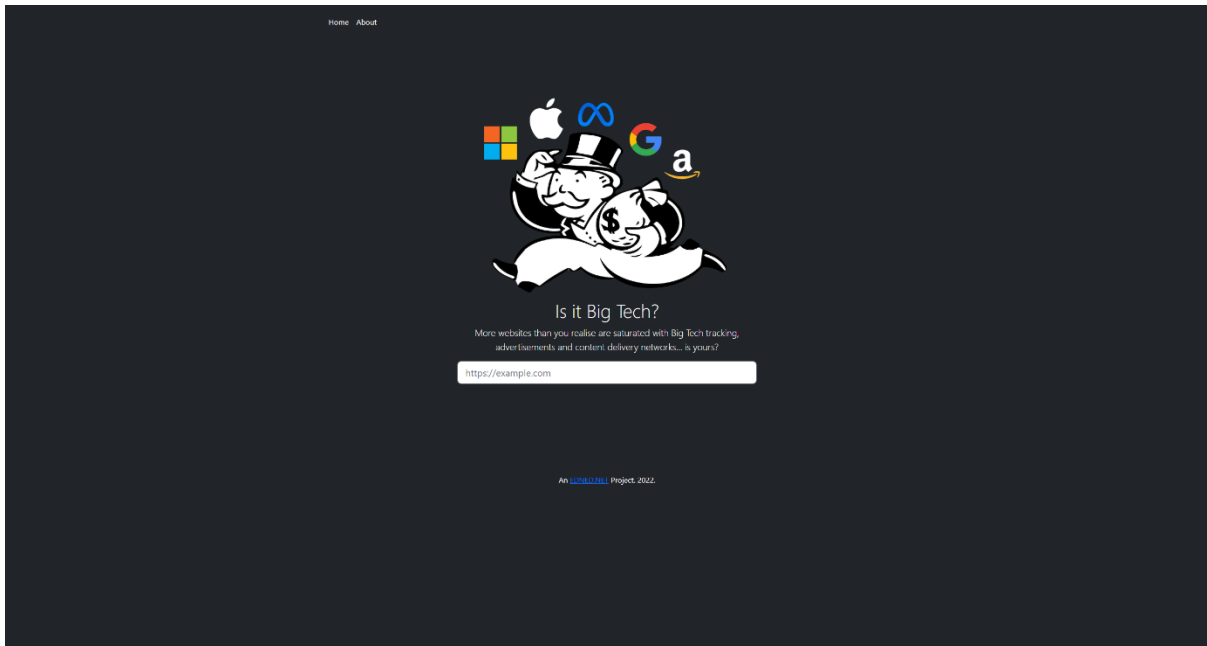


Figure 35: IsItBigTech - Index (Home)

The above page is what users will see when navigating to the website and is where all the backend code returns its data to. The user should enter their desired URL into the input field and press Enter/Return. Once the desired data is received, this will then be rendered under the input text field.

### 5.2.4.2 About

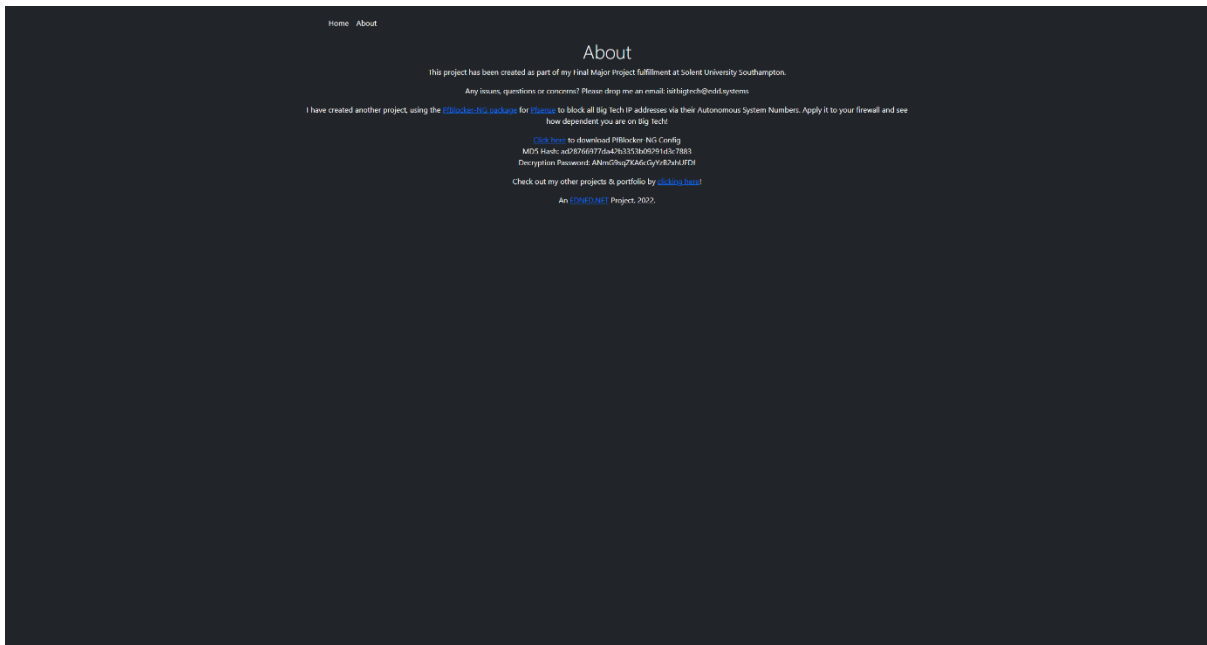
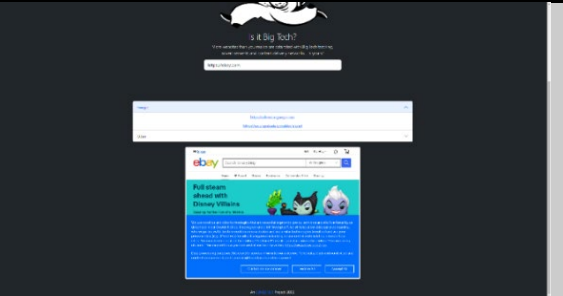
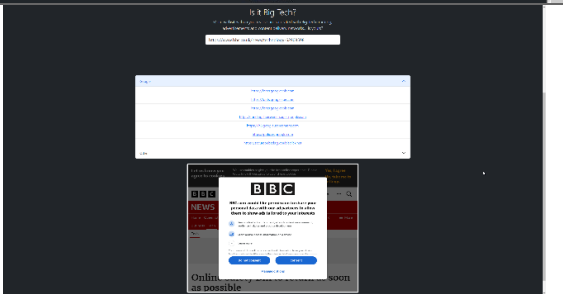
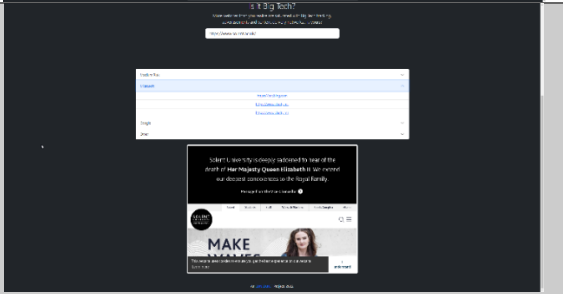


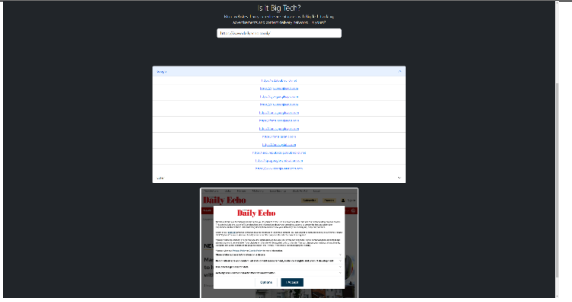
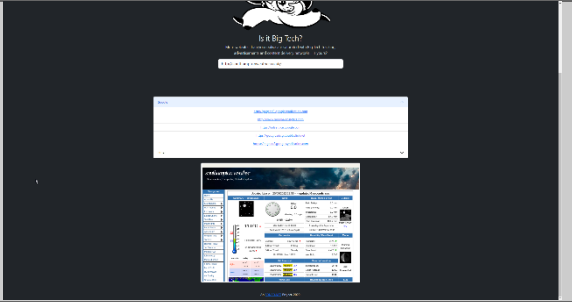
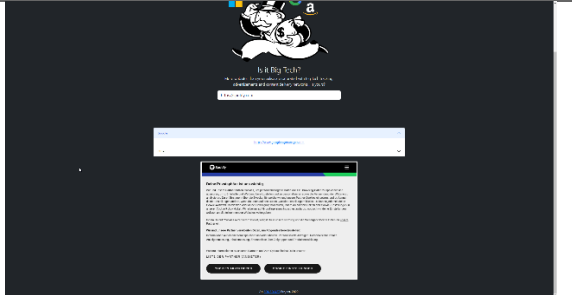
Figure 36: IsItBigTech - About

The About page is simply for informational purposes only, with some contact information and information about the project.

### 5.2.5 TESTING

The purpose of this testing section is to check that the app worked as it should have. This section tests 10 various popular websites and the results entered are supplied by the application. Each entry is dated as these sites will continue to change over time.

TEST #	Date Tested	Website Tested	Big Tech Found?	Big Tech Connections Found	Additional or Essential Content?	Site Render
001	2022-09-02	<a href="https://ebay.com">https://ebay.com</a>	Yes	<a href="https://adservice.google.com">https://adservice.google.com</a> <a href="https://securepubads.g.doubleclick.net">https://securepubads.g.doubleclick.net</a>	Additional	
002	2022-09-02	<a href="https://www.bbc.co.uk/news/technology-62908598">https://www.bbc.co.uk/news/technology-62908598</a>	Yes	<a href="https://fonts.googleapis.com">https://fonts.googleapis.com</a> <a href="https://fundingchoicesmessages.google.com">https://fundingchoicesmessages.google.com</a> <a href="https://lh3.googleusercontent.com">https://lh3.googleusercontent.com</a> <a href="https://policies.google.com">https://policies.google.com</a> <a href="https://securepubads.g.doubleclick.net">https://securepubads.g.doubleclick.net</a>	Additional	
003	2022-09-03	<a href="https://www.solent.ac.uk">https://www.solent.ac.uk</a>	Yes	<a href="https://bat.bing.com">https://bat.bing.com</a> <a href="https://www.clarity.ms">https://www.clarity.ms</a> <a href="https://www.googletagmanager.com">https://www.googletagmanager.com</a> Other Medium Risk: <a href="https://analytics.tiktok.com">https://analytics.tiktok.com</a> <a href="https://script.infinity-tracking.com">https://script.infinity-tracking.com</a> <a href="https://tr.snapchat.com">https://tr.snapchat.com</a>	Additional	

004	2022-09-06	<a href="https://www.dailyecho.co.uk">https://www.dailyecho.co.uk</a>	Yes	<a href="https://ad.doubleclick.net">https://ad.doubleclick.net</a> <a href="https://ajax.googleapis.com">https://ajax.googleapis.com</a> <a href="https://fonts.gstatic.com">https://fonts.gstatic.com</a> <a href="https://fonts.gstatic.com">https://fonts.gstatic.com</a> <a href="https://securepubads.g.doubleclick.net">https://securepubads.g.doubleclick.net</a> <a href="https://tpc.googlesyndication.com">https://tpc.googlesyndication.com</a> <a href="https://www.google-analytics.com">https://www.google-analytics.com</a>	Additional	
005	2022-09-06	<a href="http://southamptonweather.co.uk">http://southamptonweather.co.uk</a>	Yes	<a href="http://pagead2.googlesyndication.com">http://pagead2.googlesyndication.com</a> <a href="http://www.google-analytics.com">http://www.google-analytics.com</a> <a href="https://adservice.google.com">https://adservice.google.com</a> <a href="https://googleads.g.doubleclick.net">https://googleads.g.doubleclick.net</a> <a href="https://pagead2.googlesyndication.com">https://pagead2.googlesyndication.com</a>	Additional	
006	2022-09-07	<a href="https://spotify.com">https://spotify.com</a>	Yes	<a href="https://www.googletagmanager.com">https://www.googletagmanager.com</a>	Essential	

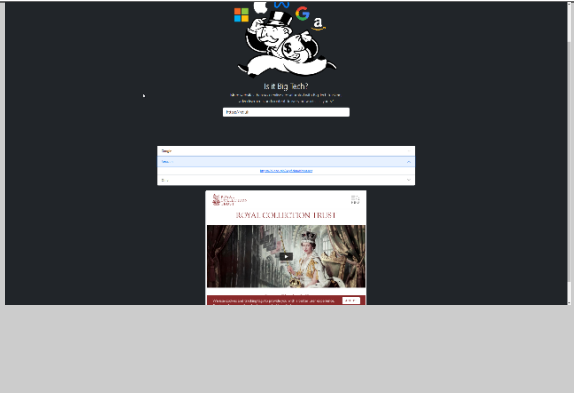
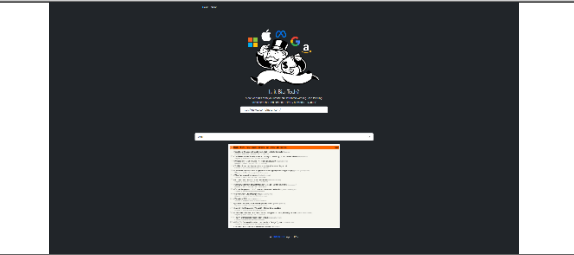
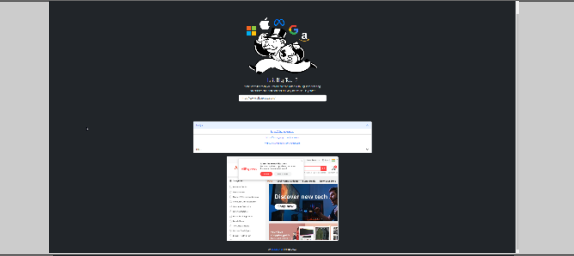
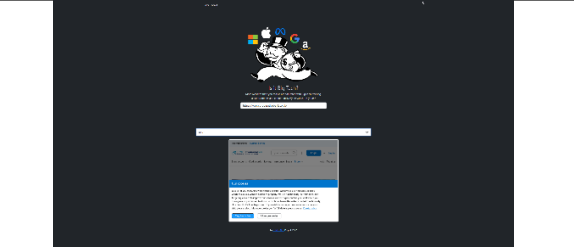
007	2022-09-08	<a href="https://rct.uk">https://rct.uk</a>	Yes	<a href="https://d1azc1qln24ryf.cloudfront.net">https://d1azc1qln24ryf.cloudfront.net</a> <a href="https://ajax.googleapis.com">https://ajax.googleapis.com</a> <a href="https://developers.google.com">https://developers.google.com</a> <a href="https://googleads.g.doubleclick.net">https://googleads.g.doubleclick.net</a> <a href="https://www.google-analytics.com">https://www.google-analytics.com</a> <a href="https://www.googleadservices.com">https://www.googleadservices.com</a> <a href="https://www.googletagmanager.com">https://www.googletagmanager.com</a>	Essential	
008	2022-09-10	<a href="https://news.ycombinator.com">https://news.ycombinator.com</a>	No	None	N/A	
009	2022-09-10	<a href="https://www.aliexpress.com/">https://www.aliexpress.com/</a>	Yes	<a href="https://www.google-analytics.com">https://www.google-analytics.com</a> <a href="https://www.googletagmanager.com">https://www.googletagmanager.com</a>	Essential	
010	2022-09-11	<a href="https://www.co-operativebank.co.uk/">https://www.co-operativebank.co.uk/</a>	No	None	N/A	

Table 4: IsItBigTech Site Dependency Testing

## 6. MITIGATIONS & RECOMMENDATIONS

This section will explore existing issues with Big Tech Dependency in more depth and potential mitigations and recommendations to parallel them in the form of three subsections, legal measures, adaptability & resilience, and education.

### 6.1. LEGAL MEASURES

The current legal space surrounding Big Tech dependency could be described as, for want of a better word, mayhem. There is a general lack of widespread awareness and understanding of issues.

#### 6.1.1. FORCE MAJEURE

Millions of businesses worldwide depend on Big Tech services to operate large proportions of their businesses, using cloud-hosted servers, colocations, or storage spaces, for example. Despite this, there is no legal requirement for businesses to have backup solutions, and more importantly, a lot of smaller businesses cannot afford additional services or mitigation plans.

For decades, legal documents and contracts have always had a 'Get-Out-Of-Jail-Free' clause which could prevent either party from having to pay legal damages due to an event out of their control which cannot be anticipated for, interrupting the signed agreement, usually with the keywords "outside of control". An example of one of these clauses is: "The College will not be liable to you for any loss suffered as a result of events that happen outside of our control such as natural disasters, extreme weather, or events which include, but are not limited to, industrial action, staff illness, terrorist attacks, political unrest, civil disorder, pandemic or loss of essential services." (LawInsider, 2022). The key is to notice the "not limited to" phrase, which relieves the contractor of an endless list of disruptions, so long as they cannot be controlled and/or prevented by them. These such events are known legally as 'force majeure', a French term that literally means 'greater/superior force'.

When an organisation contracts their systems to a Big Tech provider (such as Amazon Web Services, Microsoft Azure, Google Cloud), if any interruptions were to occur which cause a business to prevent fulfilling a legal contract such as an estate agent finalising a property sale, they have the legal right to claim 'force majeure', legally placing the outage of their systems in the same realm of 'acts of God', due to their inability to control the situation. In most cases, the Big Tech company itself is also immune from legal action as they write a similar clause within their SLA contracts, which are carefully crafted by large teams of lawyers. For an example, an extract from the AWS agreement states:

"WE AND OUR AFFILIATES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION" (AWS, 2022).

As an example of force majeure, if a service provider such as University was unable to provide their services to their students because of an outage of services provided by Microsoft, the students would understandably be annoyed at the situation and would want to act, especially if this was a prolonged outage, such as taking them to court for a partial refund of fees. The same force majeure clause would be cited to remove responsibility of this issue, "our hands were tied, we were unable to do anything".

### 6.1.2. LEGISLATORS & REGULATORS

Legal resilience against Big Tech is on the roadmap of legislators and regulators, as we have seen with the European Union and their ongoing efforts with the establishment of the Digital Markets Act (Article 114 of the TFEU), due to come into force in Spring 2023 (Lomas, 2022). However, these efforts may not prove to be enough in the long term and there's definite room for increased awareness of the risks surrounding the use and reliance on Big Tech products and services, especially for businesses.

One organisation at the forefront of the issues is the FSFE (Free Software Foundation Europe) charity is hugely focused on the issues that Big Tech creates, focusing on the rights to use, understand, adapt, and share software. They make it clear that these rights "help support other fundamental rights like freedom of speech, freedom of press, and privacy." (FSFE, 2022). They were founded in 2001 and are at the forefront of the free software movement within Europe, raising awareness of the issues at hand "it is important that this technology empowers rather than restricts us" (FSFE, 2022).

In May 2022, the UK Government set out plans on how the new Digital Markets Unit (DMU) will tackle dominance from major firms, with plans of fining companies up to 10% of their global turnover for breaches if they fail to comply with the rules. It also stated that the new watchdog would "be able to ensure fair prices for content in disputes between powerful platforms and content providers such as news publishers and advertisers" (Philip, 2022). Despite the claims of the press release, the UK Government has not confirmed when it expects to empower the DMU.

In the report titled Investigation of Competition in Digital Markets released by the US Subcommittee in 2020 investigated the Big Tech domination. Their key recommendations (in short) were:

- Restore competition in the digital economy by reducing the conflicts of interest through structural separations and line of business restrictions, implementing rules to prevent discrimination, favouritism and self-preferencing, promoting innovation through interoperability and open access, reducing market power through merger presumptions, creating an even playing field for the Free and Diverse Press and prohibiting abuse of superior bargaining power and require due process.
- Strengthening the Antitrust Laws by restoring the Antimonopoly Goals of the Antitrust Laws, invigorate merger enforcements, rehabilitating monopolisation laws, and adding additional methods to strengthen the Antitrust laws.
- Strengthening Antitrust Enforcement by congressional oversight, agency, and private enforcement.

(Rutkin et al., 2020)

The USA has since released the "Stronger Online Economy: Opportunity, Innovation, Choice" legislative package suite of acts which are aligned with the recommendations in the report, in June 2021, after the 16-month investigation into the Big Tech firms, which includes 5 new Acts:

- American Innovation and Choice Online Act - prohibits discriminatory conduct by dominant platforms, including a ban on self-preferencing and picking winners and losers online.
- Platform Competition and Opportunity Act - prohibits acquisitions of competitive threats by dominant platforms, as well acquisitions that expand or entrench the market power of online platforms.

- Ending Platform Monopolies Act - eliminates the ability of dominant platforms to leverage their control over across multiple business lines to self-preference and disadvantage competitors in ways that undermine free and fair competition.
- Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act - promotes competition online by lowering barriers to entry and switching costs for businesses and consumers through interoperability and data portability requirements.
- Merger Filing Fee Modernization Act - updates filing fees for mergers for the first time in two decades to ensure that Department of Justice and Federal Trade Commission have the resources they need to aggressively enforce the antitrust laws

(Albert, 2021)

These acts are very promising and if they come to fruition and are implemented correctly, could certainly overturn damage done by Big Tech. With careful execution, these acts could improve competition, increase innovation, and benefit consumers within the digital markets. It is important to note that legislation does not always translate into real laws that are effective and these bills still need to pass the US Congress – so despite the investigation and creation of the proposed bills, the US will be behind the EU with their Digital Markets and Digital Services Acts, and their method of implementation working from the ground up.

### **6.1.3. EXISING LEGAL INADVERTANCE**

Big Tech services are so tightly integrated and normalised in all parts of modern society that making the decision to not use them would be easy for anyone, especially in any career that involves the use of digital technology. Not because it is difficult to use alternative options, but because of the expectation of these products with limited interoperability for alternatives.

As an example, if someone were to speak to a solicitor about their concern for privacy invasion from the use of Big Tech services within their workplace, and ask what they could do about it, the current answer, depending on your job and the requirement for using the technology, would be something along the lines of “not a lot”. Of course, this would vary hugely depending on the employer and the nature of businesses, but most businesses have a strict set of products.

The previous force majeure clause opens some questions regarding responsibility for service outages and the effects on businesses, especially those in the tech industry such as service providers and cloud computing providers. These kinds of businesses should have a reasonable expectation that services are going to go down and things will go wrong, therefore, not able to supply customers with service expected. Potential clients should check force majeure contract clauses to ensure it “includes nothing that is (or should be) within the reasonable control of the cloud service provider.” (Lumley-Savile, 2012)

## 6.2. ADAPTABILITY & RESILIENCE

### 6.2.1. RESILIENCE – THE CUSTOMER/CONSUMER RESPONSIBILITY?

Should resiliency responsibilities lie in the hands of the consumer or customer to manage?

A large majority of those who use Big Tech services today are not equipped with the skills to transfer their data elsewhere, and companies have proven to make this difficult for their customers to transfer data elsewhere, known as data portability.

In a hypothetical situation where Gmail did not work either partially or fully for multiple days on end and is using severe disruption to the user, they would understandably become annoyed and would want to do something about it and would begin looking for alternative options.

Google has made it available for their users to download their data held by them in a data readable format (Google, 2022), however, to transfer and port this data to other services, it will require a degree of IT literacy to transfer correctly to the new application.

The EU's new Digital Markets Act is working on forcing Big Tech to make their data portability easier to setup and make a full requirement for all companies, "data portability includes the right of the data subject to receive the personal data concerning him or her, which he or she has provided to a controller, and the right to transmit those data to another controller" (EDPS, 2021). It is essential that the ease of data exportation and portability is closely legislated to ensure that users with little knowledge of IT can make a fully informed decision to switch without being inhibited by seemingly difficult steps to opt-out and download their data.

### 6.2.2. THE FOUR RS

You read the subheading correctly. Most people have heard of the 3 Rs in terms of waste management, "Reduce Reuse Recycle" (Reduce Reuse Recycle, 2022). This remit can be closely aligned with the usage and consumption of products and services, but at the very top of the upside-down triangle (both literally and theoretically), we should consider the 4<sup>th</sup> R – Refuse.

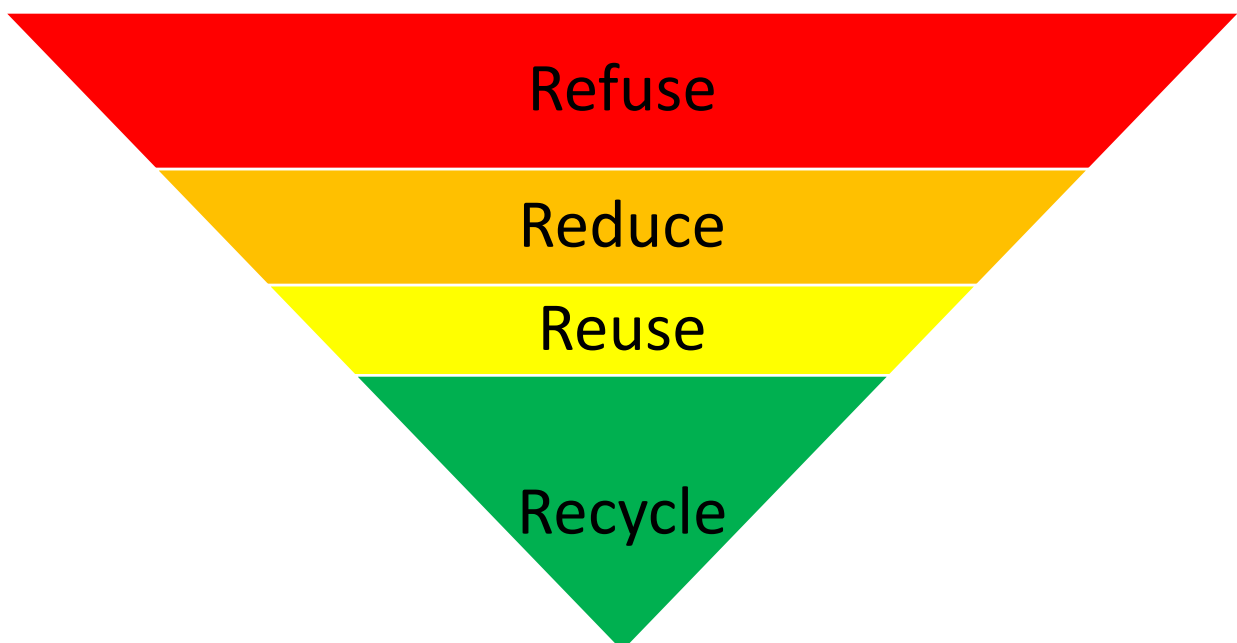


Figure 37: The 4 Rs



#### **6.2.2.1. Refuse**

Refuse is the pre-emptive piece of the puzzle. People should use due diligence to ensure that the product or service being offered to them will not make them highly dependent in the first place. Questions should be asked, such as “What will this product/service do for me?”, “Can I take my data out and move to another provider easily?”.

#### **6.2.2.2. Reduce**

If a business/person finds that they are highly dependent on a product or service and do not have any alternative or redundancy solutions, they should do so if it is essential. Once correct mitigations have been put in place, users should gradually reduce their usage until they become less dependent on it, and eventually, not dependent at all.

#### **6.2.2.3. Reuse**

‘Reuse’ in this context is really about adaptability and control and finding new ways to make products work for you, rather than the other way round, if applicable.

A good analogy which is reflective of the way we find ourselves using Big Tech services as a wider population is a book called ‘Who Moved My Cheese?’ by Spencer Johnson. Briefly, the book follows mice that live in a maze. They have learned the way to ‘Cheese Station C’ because they became dependent and ignorant in the fact that cheese would always be waiting there for them each morning. One day, it isn’t. The mice don’t want to look elsewhere for other cheese, and are uncertain, with a fear of failure and getting lost. They still returned to Cheese Station C despite there being no cheese because it was familiar to them and within their comfort zone (WISDOM FOR LIFE, 2020). This is directly representative of the way we consume tech products – people tend to use things that have always worked for them in the past and this is what enables Big Tech to exploit people.

#### **6.2.2.4. Recycle**

Rather than recycling old habits of reliability, people should exercise caution and ensure they are defended from future harm – the digital space is becoming increasingly volatile in terms of products and services changing, everything in Big Tech gets updated from a user interface point of view.

Ensuring as little dependence as possible is key.

### **6.2.3. KILLER ACQUISITIONS**

It is no secret that Big Tech acquire smaller businesses and competition from buying them out, known as “killer acquisitions”, which has come under the eye of the antitrust community. Big Tech have bought out over 600 companies in the last 30 years (See appendix B – Big Tech Acquisitions). 175 of those acquisitions have been between 2015 and 2017 (Pérez De Lamo, 2021) Not only does this destroy the competition market, but it has huge effects on users, who are reliant on these products and services. It costs time and money to learn a new skill, especially in the business sector, and this can be fatal for smaller businesses.

### **6.2.4. DEFENCE FROM FUTURE HARM**

Lessen dependency. The more dependencies a person or business has, the higher risk they are of being potentially harmed in the future, for several reasons such as sudden deprecation of products by other organisations, outages, sudden contract price rises, change in functionality, etc. The same principles for defence apply for protecting territories from threats, and resilience when considering

assets such as the UK Power Grid infrastructure. To defend from future harm, more mitigations/backups and independent operation outputs the highest degree of resilience against external harms.

Developers also have a role to play in the creation of applications by ensuring that the dependencies used are trustworthy and non-malicious. Malicious packages are always being found within programming languages, which have been found to be widely, known as supply chain attacks. In a latest report, an additional 10 malicious python packages were exposed, “The increasingly common discovery of fake, malicious packages is moving repositories to act” (Purdy, 2022)

The Pearl programming motto, TIMTOWTDI, simply means “There's more than one way to do it”. The language was created with this very idea in mind (C2, 2014). On the contrary, part of Python’s Zen is “There should be one-- and preferably only one --obvious way to do it”, though this is questionable given the number of packages found to be malicious within the Python space. Having multiple packages that achieve the same goal is ultimately what supports the drive of competition. Extremely brittle product development can lead to further harm of businesses.

## **6.3. EDUCATION**

### **6.3.1. ARRIVAL THROUGH POOR EDUCATION**

Big Tech covers a large space with a vast number of products and services, from industry cloud hosting to social media, affecting all age groups, from children to adults, and all industries, from gardeners to cyber security engineers. Cyber security and awareness of technology is no longer a professional issue, it is a civil one – and has been for many years.

However, a lot of the education on cyber security up until this point has proven to be poor and deceptive, with a lot of misinformed junk ‘information and advice’ such as guides on “How to stay safe online” funded by consortiums of ISPs, smartphone manufactures, social media companies and data analytic firms (Farnell, 2021).

Big Tech’s primary target audience is young children – the very people who not only know little about technology but are incredibly vulnerable. Therefore, it is of utmost importance that young people are educated on the security and privacy risks surrounding their data online, “Data gathered on young people, which can include information about their race, ethnicity, religion, income, and network of friends, can be used in discriminatory ways that may harm their access to opportunities and services. It is estimated that online advertising firms hold 72 million data points on the average child by the time they reach the age of 13, allowing marketers to target children's vulnerabilities with extreme precision” (Stancil, 2022).

### **6.3.2. PRODUCTIZATION**

Education models have shifted to teaching products rather than skills and principles. For years, schools, colleges, and universities across the world have spent far many more hours teaching products like the Microsoft Office rather than teaching skills like programming, security, *real* online safety, and other essential skills that educate people to ensure technology is working for them, and not the opposite way around, “A decent education in computer science is increasingly looking radical and subversive, and must be obtained outside of, despite and not through, the official education system.” (Farnell, 2021).

Productization is not just about the products being taught, but the people becoming the products, “Facebook has no financial interest in telling the truth. No company better exemplifies the internet-age dictum that if the product is free, you are the product.” (Lanchester, 2017)

### **6.3.3. POLARISED AND MONOPOLISTIC MARKET**

“Other brands and services are available” is a term we hear a lot on BBC television and radio broadcasts (BBC One, 2018). They must utter this phrase because they are not allowed to endorse or advertise brands due to their public funding from TV Licencing, and lets the audience know that there are other brands and similar products available, it’s a free market after all – right? Unfortunately, this isn’t quite the case when it comes to digital technologies and services.

The existing market of software and digital services has become so polarised and monopolised by Big Tech that many businesses and individuals cannot see any other available alternatives on the market, and do not always have the ability or the availability to do something about transitioning away from the dominant platforms, due to the complexity of exporting and interoperability of data (see section 6.2.3. Killer Acquisitions above). It goes without saying that Big Tech companies of course would like to retain as many customers as possible, “Our belief that Big Tech like Google and Facebook is ‘safe’, because ‘everybody else is doing it’, is seductive but false. Ironically, when it comes to data abuses, there is no ‘safety in numbers’. The more of us there are, the more attractive a target we all make.” (Farnell, 2021).

The general population should be reminded to exercise their right to search and be aware of alternative products and services, whether for personal or business use. Keep an open mind and be aware of alternative options.

### **6.3.4. ORGANISATIONAL INTERVENTION**

The education problem requires involvement from government and state organisations in the interests of national security for countries and civil societies, responsibility should lie with the Department for Education in the UK. The government should educate children about protecting their privacy online, and general cyber security. This is because, as the world becomes increasingly digitalised, it is important that children are aware of the risks they face while navigating the internet. The government should be responsible for educating children about these things, and not big tech corporations.

There is no point in leaving this responsibility in the hands of Big Tech. They have their own exploitative agenda, largely lead by monetary and data profiteering. They are the very last organisation that should be teaching this subject, ending in providing inaccurate information. If they were to teach people about the dangers of themselves, it would be the equivalent of a news reporter describing a police sketch of a wanted criminal which looks identical to them, which happened on ABC News in 2011 (ABC News, 2011).

### **6.3.5. THE TECH SECTOR & DEVELOPERS**

The tech industry is an ever-growing and influential sector of the economy. It has a disproportionate impact on the world, but it also has its own set of problems.

The Tech Sector in general is becoming low educated with the acceleration of product-based training courses, offered by companies like Amazon and Microsoft. Employees working in this sector become \*Insert Big Tech Company\* Certified rather than shifting the focus on transferrable skills. Though, it is understandable that this would occur within the Tech Sector when so many companies rely directly upon Big Tech hosting and other cloud-based products – when potential employees are trying to get a job and becoming Microsoft/AWS/Google Cloud certified increases their chances of

getting a job within a certain organisation because they use those products, of course this would put the applicant above the rest who do not have this.

CompTIA is a non-profit organisation that issues professional certifications for general competency in three main sectors, foundation IT knowledge (A+), Networking (Network+) and Cyber Security (Security+), as well as tens of other specific certifications in cyber security and other sectors in the industry (CompTIA, 2022). Using this approach encourages general transferable knowledge which is a lot more valuable and allows professional development of skills over a multitude of products, enforcing thinking, information exchange and innovation between professionals, even if their companies are using different products.

According to PCMag (2022), The top 3 paying IT certifications are all directly related to Big Tech, as it currently stands:

- 3) AWS Certified Solutions Architect – Associate (average of \$159,033 per annum)
- 2) Google Cloud Professional Cloud Architect (average of \$169,029 per annum)
- 1) Google Cloud Professional Data Engineer (average of \$171,749 per annum)

Informed opinions from the seeming minority of forward-thinking engineers and developers within the industry are usually disregarded because there is no incentive to change the existing structure of businesses. A quote by Upton Sinclair (1934), “It is difficult to get a man to understand something when his salary depends upon his not understanding it.”

#### **6.3.6. THE NEXT GENERATIONS**

Unlike a complex and deeply established international technology sector, it is thought that the general population would be much more malleable to change. Technology is constantly changing and evolving anyway. According to a poll by the Independent, the average adult “will spend 34 years of their life looking at screens”, with “64 per cent admitted they would not know what to do without their screen time” (Elsworthy, 2020). These are shocking statistics considering our choice over technology is minimal when compared to choices over things such as personal health, clothes, careers, friends, etc. Making informed technology choices must become an essential component of our roles and responsibilities as human beings, “the best approach is for citizens to be highly conscious and well-informed about the impacts of their technology choices when deciding how they live and what they buy. It is a huge behavioral change.” (Grossenbacher, 2020)

As part of this research, the Department for Education were contacted for a comment on how they are educating the next generation on the risks of cyber security awareness and digital self-defence, and general risks surrounding Big Tech companies. See Appendix A – Secretary of State for Education for the full letter correspondence. Most importantly, A Townsend acknowledged in their reply to the letter growing concerns regarding harmful online activity and content mentioning that it “can be particularly damaging for children and there are growing concerns about the potential impact on their mental health and wellbeing.” To follow this, they also mention that the new Online Safety Bill will “make the UK the safest place to be a child online”, claiming that “all companies in scope of the legislation will have to do far more to address illegal content and activity on their service”, as well as putting in place “safety measures to protect them from harmful content like pornography, and behaviour such as bullying”. Moreover, the new Bill will empower Ofcom to “take enforcement action, including large fines, against companies that fail to comply with these duties”.

It is hoped that the new legislation will bring some important change for children’s protection using Big Tech services, and whilst this does not directly tackle the issue of Big Tech, it is certainly a step in the right direction to protect the next generations from cyberbullying, exploitation and more.

## 6.4. “MR ROBOT” SCENARIOS

This section could be considered by some to have an enigmatic subheading, though this is rather appropriate. Mr Robot is a drama TV Series released in 2015, created by Sam Esmail, which is well known within the industry. In short, the series follows the main character, Elliot Alderson, a cyber-security engineer by day and a vigilante hacker by night. The show explores what would happen if a company became too big and powerful and what would happen if it had too much control over people's lives. In the show, Elliot's hacker group performs the 'world's largest redistribution of wealth'. The show's portrayal of “Evil Corp” as a villainous power-hungry company can be seen in its slogan: "You are not safe." It also portrays them as a company that thrives on exploiting people's data for their own good.

Whilst the show has a rather theatrical outcome, it offers a rather worryingly pragmatical insight into possible scenarios we could find ourselves in as we look into the near future, when aligning the plot of the programme with the current direction of the technology industries and the monopoly of the Big Five companies.

This section will explore the three scenarios that are most likely to be experienced when “the wheels fall off”, so to speak.

### 6.4.1. SCENARIO ONE — INEVITABLE FAILURES

The first scenario will see major sectors of Big Tech beginning to fail. As of 2022, we already seeing this happen more frequently than would be desired, with major outages across many platforms, such as Amazon Web Services, Microsoft Azure/Office, Google, etc. This is already having large impacts on society, even though in most cases the outages are short-lived.

The main difference looking into the future is that as the frequency of these failures will inevitably increase and society becomes more dependable on them, the impact that it has on society will only continue to worsen – this is inevitable when individuals and businesses begin to rely on only a few companies to serve most of the world data.

It is at that point in time the response of Governments, companies, and individuals will define the outcome of this situation.

The governments could take action to increase competition such as enacting legislation which limits centralisation and enhances choice of services and more. This would allow other companies to access the existing market, which is currently saturated by Big Tech. With consumers able to This would naturally increase resilience of technologies.

This is a corrective course that does not require much imagination. It would essentially just be proof that our “system” is working, in terms of capitalism, democracy and general markets.

If Big Tech products begin to get too big to be effectively upheld, their failure will cause anger and frustration with people. They will look for alternative products and services and the general landscape will correct itself and straighten out as expected.

The EU are leading the way with this with their current Digital Markets Act proposal under Article 114 of the TFEU. Whilst this is currently a slow and ineffective development, it is leading by example and anti-monopoly strategies do work and will be one of the better ways to regain balance, security, and reliability.

#### 6.4.2. SCENARIO TWO — GOVERNMENT/POLITICAL INVOLVEMENT OF BIG TECH

The most likely scenario is that Big Tech continue to gain money and power to a point where many governments across the world are manipulated and controlled by them. As touched on earlier, there is a huge lack of understanding already from the US Government surrounding the risks with Big Tech companies. Big Tech’s attitude towards the rules of law, legislation, and privacy has already been proved by the way that these companies have acted in the past and present. Many of these companies have received multiple fines from EU countries for countless reasons, of which they would rather pay than abiding by the rule of law like everyone else, which clearly gives off a “it is not important to us” and “might is right” attitude. With more than \$30 billion worth of antitrust fines issued to Big Tech since 2015 (Fitri, 2022), their ability to buy themselves their own path is scary and only going to get much worse.

Some examples of fines issued to Big Tech organisations:

Company	Issued By	Fine Reason	Date	Fine Amount	Source
<b>Amazon</b>	EU Commission	Amazon's processing of personal data didn't comply with EU rules	30 <sup>th</sup> July 2021	\$887 million	(Reuters, 2021)
<b>Amazon</b>	Italy's antitrust watchdog	Leveraging its dominant position in the Italian market for intermediation services on marketplaces to favour the adoption of its own logistics service - Fulfilment by Amazon	9 <sup>th</sup> December 2021	\$1.3 billion	(Pollina et al, 2021)
<b>Apple</b>	EU Commission	Abusing its market position for contactless smartphone payments	2 <sup>nd</sup> May 2022	\$36.6bn (ongoing – Apple promised to engage with EU)	(BBC News, 2022)
<b>Apple</b>	Brazilian Government	Selling iPhones in Brazil without a power adapter	7 <sup>th</sup> September 2022	\$2.4 million & ban on selling phones without charger in Brazil	(BBC News, 2022)
<b>Apple</b>	DGCCRF	Deliberately slowing down older iPhone models without making it clear to consumers	7 <sup>th</sup> February 2020	€25 million	(BBC News, 2020)
<b>Google</b>	EU Commission	Using the Android platform to cement its search engine's dominance.	14 <sup>th</sup> September 2022	€4.125 billion	(BBC News, 2022)
<b>Google</b>	EU Commission	Failing to negotiate "in good faith" with news organisations over the use of their content	13 <sup>th</sup> July 2021	€500 million	(BBC News, 2021)
<b>Google</b>	EU Commission	Abusing dominance as search engine by giving illegal advantage to own comparison shopping service	27 <sup>th</sup> June 2017	€2.42 billion	(European Commission, 2017)
<b>Google</b>	EU Commission	Abusive practices in online advertising	20 <sup>th</sup> March 2019	€1.49 billion	(European Commission, 2019)

<b>Meta / Instagram</b>	EU Commission	Mishandling children’s user data, failing to protect children’s privacy.	5 <sup>th</sup> September 2022	\$403 million	(Sevilla, 2022)
<b>Meta / Facebook</b>	UK Competition Regulator, CMA	Deliberate failure to comply with UK Regulator - "consciously" refused to report all required information during investigation of Giphy.	20 <sup>th</sup> October 2021	\$70 million	(UK Government, 2021)
<b>Meta / Facebook</b>	US Federal Trade Commission & UK's data protection watchdog	Allowing Cambridge Analytica access to the private data of 87+ million users.	30 <sup>th</sup> October 2019	At least \$10 billion + £500,000	(Holt, 2019)
<b>Microsoft</b>	EU Commission	Failing to promote a range of web browsers, rather than just Internet Explorer, to users in the EU.	6 <sup>th</sup> March 2013	€561 million	(BBC News, 2013)

*Table 5: Big Tech Fines*

There are countless other breaches of laws and regulations and fines, and a strong possibility of others that have not been picked up on by any watchdogs yet, but this offers some insight into the attitudes to that Big Tech corporations have; knowing that they monopolise the markets and user data. Entries in the table above highlighted in red are some of the biggest fines ever issued.

As a prime example, Meta allegedly paid \$4.9bn more than necessary to the US Federal Trade Commission in a settlement over the Cambridge Analytica scandal to protect Mark Zuckerberg, “Facebook has proved that they are prepared to pay almost any sum of money to avoid their executives answering these questions. This settlement comes on top of the \$5bn they already paid the FTC.” (Townsend, 2022)

### 6.4.3. SCENARIO THREE — SELF-DEVOURMENT

The third possible scenario is that Big Tech systems and services could consolidate and shrink until they become completely dysfunctional. This is not a new concept and has happened many times before in human history.

Thomas Malthus, an English economist born in 1766, observed in his book, *An Essay on the Principle of Population* (1798), that humans tended to focus on population growth rather than maintaining a higher standard of living – this is known as “Malthusianism”. The common principles of this theory apply to Big Tech’s existence today, with their ‘buy and kill’ tactics, known as ‘killer acquisitions’ (Ederer, 2021), and constant creation and abandonment of products and services without care of their users.

Edvin Linden has created a website named “Killed by Tech”, which is an excellent visual timeline representation of the discontinued products from Apple, Google, and Microsoft since 1996 (Linden, 2022).

The path in which Big Tech conglomerates are currently on is largely representative of the historic Bronze Age collapse. It was never thought that the civilised world of the Bronze Age would ever cease to exist, but this is exactly what happened, “After centuries of brilliance, the civilized world of the Bronze Age came to an abrupt and cataclysmic end. Kingdoms fell like dominoes over the course of just a few decades.” (Cline, 2014). We now know that the critical flaws of this time that led to its

collapse were centralisation, specialisation, complexity, and top-heavy political structures, as explored further in Cline's book, *1177 B.C.: The Year Civilization Collapsed*.

It is important to note that the main reason Big Tech are comparable to an event such as the above is due to the huge amount of dependency that society currently have on these companies to keep the world functioning, with huge business models, communication, social conformity, etc. As explored in the above projects, there aren't many websites or services that would continue working properly, if at all.

The model of Big Tech services is already incredibly delicate as they are heavily relied upon; creating a cascading failure scenario and a "domino effect" if a large enough percentage of Big Tech services were to fail for any length of time – causing the rest of the services to fail very quickly. This could create a "Black start" scenario, to the point where all internetworked systems fail at once and are unable to be restarted as they have dependencies of other services – this would cause detrimental impact to businesses, public services, global communications, and infrastructure across the planet.

An interesting comparison to make with this scenario is a black start situation of a national grid, like here in the United Kingdom. If the entire grid shut down at the same time due to a cyber-attack or any other reason, it is much more difficult to restart the grid when there's no power anywhere to initiate the process in the first place. This is what we call the "black start" recovery process, which requires a lot of electricity.

In the UK, there are a very limited number of power stations capable of a Black Start – meaning it will take a while to rebuild enough power to restart substations. The National grid believes 60% of national power demand would be restored within 24 hours of a Black Start. However, the official risk planning assumptions warn it could take 5-7 days for power to be completely restored (National Grid, 2017). This sort of event has not been planned for in terms of internet services, though there have been examples of this happening in isolated events in recent years.

In October 2021, Facebook engineers managed to pull all their BGP routes from the internet, meaning nobody was able to access any Meta-owned services for over seven hours. Employees became locked out of their offices and datacentres (Heath, 2021) because the Facebook-based security login relied on their own services and therefore made the recovery a lot more difficult. This is just one example of how agile the infrastructure is becoming just in sheer terms of outages.

No matter how successful an organisation, business, government, empire, etc. may be, their space will run out. Not in digital storage space, but societal space. This could happen for several reasons, but human history has shown that Big Tech's time in their current capacity will certainly have to change.



## **7. CONCLUSIONS**

### **7.1. PRELIMINARY SURVEY CONCLUSIONS**

From the preliminary survey and the interviews conducted with a range of people of different ages and professions, dependency on Big Tech is very high, and most people do not have contingency plans to cope with the loss of these services, in both business and personal settings. This is a big cause for concern because the dependency on their services is a direct catalyst for continuing and worsening the monopolies Big Tech hold, as they rely on this dependency to gain more money and power.

Applying the use case scenarios and the results of the preliminary survey to the firewalled labs initially will offer a good scope to analyse the direct affects this has on the users and their devices themselves, further investigating the overall share of the browsable internet Big Tech hold, even on seemingly independent websites which use Content Delivery Networks and other services from companies such as Amazon, Google, and Microsoft to deliver larger content (as discussed in Figure 1). It is important to note that these studies were conducted on a small scale initially, though it certainly offers insight and encourages the need for further research to gather more information on a wider amount of dependency cases.

### **7.2. AWARENESS THROUGH EDUCATION AND MESSAGING**

The most effective way to raise awareness of the bigger picture surrounding Big Tech is through education on the issues at large, starting from our young people to the existing adult population, and businesses, through meaningful messaging with large-reaching campaigns, backed by Government institutions, and our education system, to all age ranges.

It is hoped that if the general population were more aware of the vast problems Big Tech causes, as covered in this thesis, for cyber security of devices, personal data protection, a plethora of mental health problems in young developing minds of children, the effects on businesses worldwide, the dampening of personal choice, the vast amount of tracking deeply engrained into our internet, the immensely concerning dependency that Big Tech companies are entrusted with from millions of individuals and businesses across the world, the dominance of communication channels, and so much more – that people would begin to do something about it, rather than an “out of sight, out of mind” approach, which most people take to upsetting information that they do not want to be actively aware of.

### **7.3. CURRENT VIABLE TECHNOLOGIES & ACTIONABLE MITIGATIONS**

We have a substantial amount of current viable technologies available to allow people to detract from their dependency on Big Tech services, protecting themselves and their data, across all areas of Big Tech, and it is forever expanding. Open-source alternative applications are available for almost any type of application, from developer tools to communication, and made easily browsable for anyone through projects such as “[opensourcealternative.to](https://opensourcealternative.to)”.

By individuals and businesses making their data portable and formatted in universal standards, they can maximise their Digital Agility, and therefore their security and resiliency. Once an individual/business can reasonably say that they can rapidly enable, update, and change their digital processes, as well as being able to rapidly respond to potential problems and mitigate them whilst minimising stress without too much hassle or time, they can consider themselves to be reasonably digitally agile (Mcguire, 2020).

Open-source projects like Pi-hole are always being maintained and updated by large groups of people, as previously covered, and constantly expanded and improved upon. This is just one of millions of alternative available software packages that can be utilised at zero cost. It is becoming easier by the day, as both an individual and an organisation, to reduce dependency over time from Big Tech products and services and become a largely independent entity again.

As well as looking for alternative software solutions, people can make instant and straightforward changes to ensure resilience and data privacy.

Many applications and systems use Google's DNS Servers, even if they are not set at the device endpoint, they can be used by Internet Service Providers down the line. Changing DNS server providers is easy, and there are plenty of alternative providers available (Jelen, 2018).

VPNs can also be used, ensuring that traffic is inaccessible and not readable by Internet Service Providers, there are also hundreds of VPN providers available, each with their pros and cons (Williams 2022).

Multihoming is the practice of connecting a device to more than one network (F5, 2022). Having more than one ISP is a great way to increase resilience from outages, especially within business environments that cannot afford network outages.

Organisations, governments, and individuals are not alien to the topic of resiliency, or "Plan B", we use it in all aspects of life: transport, food chain supplies, the national grid, medications, water, communications, etc. We have become so dependent on technology as a society, though so widespread resiliency is far and few between. Current viable technologies are ready to serve the people as intended, are they ready to be served by them?

## 7.4. LEGISLATIVE IMPLEMENTATION CONCERNS

### 7.4.1. 3 STAGES OF CORRECTION

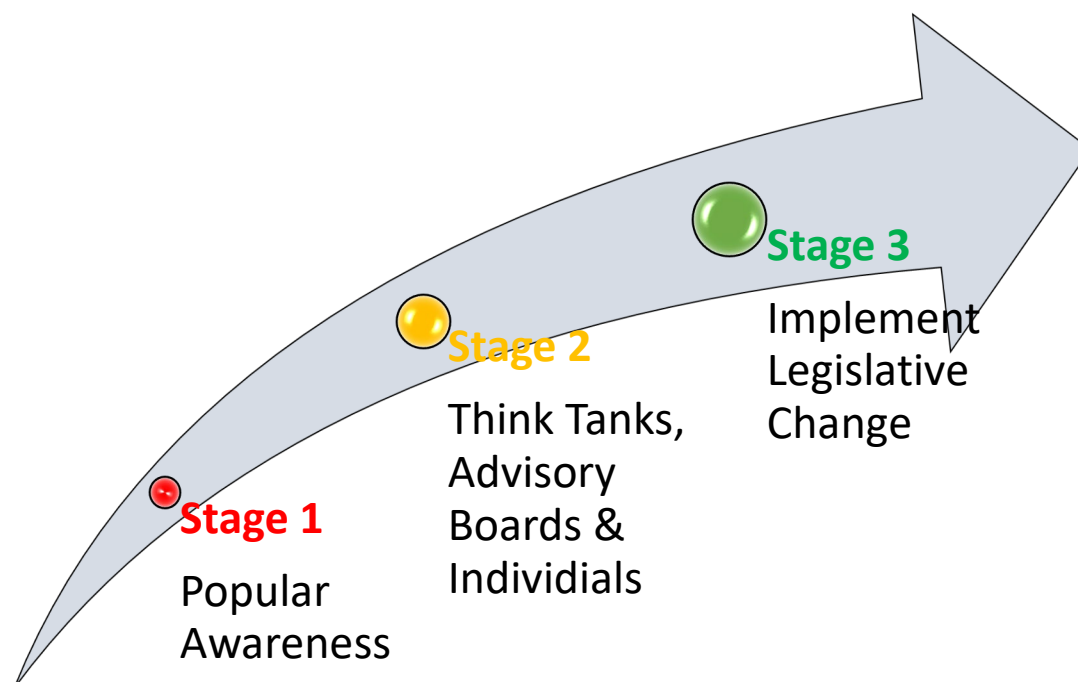


Figure 38: 3 Stages of Correction

#### **7.4.1.1. Stage 1 – Popular Awareness**

Once awareness of the wider issues surrounding Big Tech become more widely known, and there is a general understanding in society of what these issues mean for people, this is the first step to creating change. Society will feel obliged to have their say.

#### **7.4.1.2. Stage 2 – Think Tanks, Advisory Boards & Individuals**

The popular awareness will spark larger organisations, such as think tanks and advisory boards to work with groups of individuals to ensure the issues are put to writing and prepared for scrutiny by governments and legislative implementers. Complex answers and solutions to the problems raised will be compiled.

#### **7.4.1.3. Stage 3 – Implement Legislative Change**

Ministers and legislators who are prepared to act will be able to begin developing legislation utilising the answers and solutions to the problems that will enact real change to be enforced. Change of this magnitude is always a slow process, but if enough people care, it will happen.

#### **7.4.2. SHORT-TERMISM IS THE ENEMY**

Big Tech thrives from short-termism, concentrating on short-term projects and objectives for immediate profits. Making changes to laws on Big Tech services such as social media will take decades to fully implement, as we have seen from ongoing development of laws and legislation. It is the equivalent of trying to steer a large cargo ship, it requires forward thinking much further ahead to make the turn in time, this is the same as implementing new laws and regulations.

### **7.5. FUTURE RESEARCH**

This thesis only touches on what is such a large expanding issue that affects everyone, everywhere, providing they use technology – which covers a large majority of the world’s population. A few research topics that could follow from this in more detail are:

- 🚩 Awareness in Depth – Is Society aware of Big Tech’s global lasting impacts?
- 🚩 Actionable Digital Agility for Civilians – Depriving Big Tech from Its Target Audience
- 🚩 Anti-Big Tech VPNs – Protecting Users from Big Tech via Virtual Networking
- 🚩 ‘OneClick’ Digital Self Defence Applications – Simplifying & Empowering Civil Cyber Security
- 🚩 The Rise of Big Tech & our Failed Legal Systems

## 8. FURTHER READING

This section explores further reading around the subject area, in the form of both websites, tools, guides & books.

### **DIGITAL RESILIENCE FRAMEWORK – UK COUNCIL FOR INTERNET SAFETY**

**[UKCIS DIGITAL RESILIENCE FRAMEWORK.PDF \(PUBLISHING.SERVICE.GOV.UK\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672227/ukcis-digital-resilience-framework.pdf)**

The Digital Resilience Framework is a useful guide created by members of the UK Council for Internet Safety (UKCIS) to support anyone with little knowledge of security in self assessing their digital environment, content, services, and policies and working to enhance their digital resilience.

### **DIGITAL VEGAN BY DR ANDY FARNELL**

The Digital Vegan book extensively covers the issues caused by Big Tech in our society, from market monopolies and smartphone addiction to e-waste, in a comprehensive bid to raise awareness of avoiding toxic hardware, software and media in people's lives.

### **DON'T BE EVIL: THE CASE AGAINST BIG TECH BY RANA FOROOHAR**

Don't Be Evil: The Case Against Big Tech covers in depth the market dominance by Big Tech and the threats it causes to our democracies, economies, and ourselves.

### **LEDGER OF HARMS – CENTER FOR HUMANE TECHNOLOGY**

**[HTTPS://LEDGER.HUMANETECH.COM](https://ledger.humanetech.com)**

Ledger of Harms explores in a simple but informative format the issues caused by technology platforms. From the next generations, physical and mental health to effects on social relationships, it is certainly an essential resource to share and acknowledge.

### **OPEN-SOURCE ALTERNATIVE ([HTTPS://WWW.OPENSOURCEALTERNATIVE.TO](https://www.opensourcealternative.to))**

Open-Source Alternative is a tool that shows people hundreds of open-source alternative applications to proprietary SaaS platforms, in a modern and easy to use format.

### **RESILIENCE IN THE DIGITAL AGE BY FRED S. ROBERTS, IGOR A. SHEREMET**

This book explores new approaches to the resilience of socio-technological and natural-social systems in a digital world of big data, extraordinary computing capacity, and rapidly developing methods of Artificial Intelligence.

### **SYSTEM ERROR: WHERE BIG TECH WENT WRONG AND HOW WE CAN REBOOT**

**BY ROB REICH**

System Error offers a powerful account of how our lives, our politics, and our values have been reshaped by technology in ways that we are just starting to comprehend. Full of stories and insights, this remarkable book charts a path forward for creating a healthy digital future.

## 9. REFERENCES

- ABC News, 2020. Microsoft: Russian-backed hackers targeting cloud services [viewed 7 June 2022]. Available from: <https://abcnews.go.com/Technology/wireStory/microsoft-russian-backed-hackers-targeting-cloud-services-80769005>
- Albert, A., 2021. Big Tech, Big Problems, & Big Solutions: The Legislative Package to Reinvigorate Platform Competition [viewed 21 September 2022]. Available from: <https://publicknowledge.org/big-tech-big-problems-big-solutions-the-legislative-package-to-reinvigorate-platform-competition/>
- Apple., 2009. Apple Announces the New iPhone 3GS — The Fastest, Most Powerful iPhone Yet [viewed 10 September 2022]. Available from: <https://www.apple.com/uk/newsroom/2009/06/08Apple-Announces-the-New-iPhone-3GS-The-Fastest-Most-Powerful-iPhone-Yet/>
- AWS., 2018. AWS Customer Agreement [viewed 21 September 2022]. Available from: <https://aws.amazon.com/agreement/>
- BBC News., 2020. Apple fined for slowing down old iPhones [viewed 11 September 2022]. Available from: <https://www.bbc.co.uk/news/technology-51413724>
- BBC News., 2021. Google fined €500m by French competition authority [viewed 11 September 2022]. Available from: <https://www.bbc.co.uk/news/technology-57811953>
- BBC News., 2022. Brazil bans sales of iPhones without USB power adapters [viewed 11 September 2022]. Available from: <https://www.bbc.co.uk/news/technology-62833037>
- BBC News., 2022. EU accuses Apple of breaking competition law over contactless payments [viewed 11 September 2022]. Available from: <https://www.bbc.co.uk/news/business-61300874>
- BBC News., 2022. Google loses appeal over record EU anti-trust Android fine [viewed 14 September 2022]. Available from: <https://www.bbc.co.uk/news/technology-62888137>
- BBC One., 2022. Other brands are available [viewed 11 September 2022]. Available from: <https://twitter.com/bbcone/status/1009528699505520640>
- Bulao, J., 2022. How Many Companies Use Cloud Computing in 2022? [+35 Stats] [viewed 9 June 2022]. Available from: <https://techjury.net/blog/how-many-companies-use-cloud-computing/>
- C2., 2014 [viewed 20 September 2022]. Available from: <http://wiki.c2.com/?ThereIsMoreThanOneWayToDolt>
- Check Point., 2022. The Biggest Cloud Security Challenges in 2022 - Check Point Software [viewed 9 June 2022]. Available from: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/the-biggest-cloud-security-challenges-in-2022/>
- CLAYTON, J., 2022. Europe agrees new law to curb Big Tech dominance [viewed 6 June 2022]. Available from: <https://www.bbc.co.uk/news/technology-60870287>
- Cline, E H., 2014. *1177 B.C. : the year civilization collapsed*. Princeton. ISBN 9780691140896.

Cloudflare., 2021. What is a CDN? | How do CDNs work? [viewed 15 July 2022]. Available from: <https://www.cloudflare.com/en-gb/learning/cdn/what-is-a-cdn/>

Cloudflare., 2021. What is an autonomous system? | What are ASNs? [viewed 15 September 2022]. Available from: <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-an-autonomous-system/>

CNET, 2018. Google’s congressional hearing highlights in 11 minutes. YouTube

CNET, 2018. Zuckerberg explains the internet to Congress. YouTube

CNET, 2020. Everything Amazon CEO Jeff Bezos just said to Congress in 13 minutes. YouTube

CNET, 2020. Everything Facebook CEO Mark Zuckerberg just said to Congress in 16 minutes. YouTube

CNN Business., 2018. These are the most confusing questions Congress asked Zuckerberg. YouTube

Cohen, N., 2010. In *Allowing Ad Blockers, a Test for Google* (Published 2010). The New York Times

CompTIA., 2022. (IT) Information Technology Certifications | CompTIA IT Certifications [viewed 22 September 2022]. Available from: <https://www.comptia.org/certifications>

CRAWFORD, M., 2021. Big Tech’s threat to democracy [viewed 6 June 2022]. Available from: <https://unherd.com/2021/06/big-techs-threat-to-democracy/>

Ederer, F., 2021. Does Big Tech Gobble Up Competitors? [viewed 21 September 2022]. Available from: <https://insights.som.yale.edu/insights/does-big-tech-gobble-up-competitors>

EDPS., 2021. On the Proposal for a Digital Markets Act Available from: [https://edps.europa.eu/system/files/2021-02/21-02-10-opinion\\_on\\_digital\\_markets\\_act\\_en.pdf](https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf)

Elsworthy., 2020. Average adult will spend 34 years of their life looking at screens, poll claims. The Independent, 11 May

European Commission., 2019. Press corner [viewed 11 September 2022]. Available from: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1770](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770)

European Commission., 2017. Press corner [viewed 11 September 2022]. Available from: [https://ec.europa.eu/commission/presscorner/detail/en/MEMO\\_17\\_1785](https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1785)

European Parliament., 2021. Digital Markets Act: Parliament ready to start negotiations with Council | News | European Parliament [viewed 8 June 2022]. Available from: <https://www.europarl.europa.eu/news/en/press-room/20211210IPR19211/digital-markets-act-parliament-ready-to-start-negotiations-with-council>

F5., 2022. What Is Multi-Homing? [viewed 15 September 2022]. Available from: <https://www.f5.com/services/resources/glossary/multi-homing>

FARNELL, A., 2021. *Digital Vegan*. London: Applied Scientific Press

Fields, R., 2016. Happy 10th Anniversary to pfSense® Open Source Software [viewed 14 September 2022]. Available from: <https://www.netgate.com/blog/happy-10th-anniversary-to-pfsense-open-source-software>

Financial Times., 2022. The Economics of Big Tech [viewed 6 June 2022]. Available from: <https://www.ft.com/economics-of-big-tech>

FITRI, A., 2022. Can fines break Big Tech monopolies? [viewed 11 September 2022]. Available from: <https://techmonitor.ai/policy/can-fines-break-big-tech-monopolies>

FSFE., 2022. FSFE - Free Software Foundation Europe [viewed 21 September 2022]. Available from: <https://fsfe.org/index.en.html>

GARFINKEL, S., 1996. Browser Cookies are Persistent, Not Necessarily Evil [viewed 14 September 2022]. Available from: <https://www.wired.com/1996/12/browser-cookies-are-persistent-not-necessarily-evil/>

Gillard, M., 2020. Breadcrumbs [viewed 9 June 2022]. Available from: <https://www.contino.io/insights/whos-using-aws>

Google., 2022. Google Takeout [viewed 21 September 2022]. Available from: <https://takeout.google.com/>

GREENFIELD, A., 2021. We know Amazon is killing the high street, so why do we keep clicking on ‘buy now’? [viewed 7 June 2022]. Available from: <https://www.theguardian.com/commentisfree/2021/apr/26/amazon-killing-the-high-street-online-shopping>

GROSSENBACHER, J., 2020. Why we must learn to make technology a choice [viewed 22 September 2022]. Available from: <https://thehill.com/opinion/technology/490796-why-we-must-learn-to-make-technology-a-choice/>

HEATH, A., 2021. Facebook is scrambling to fix massive outage [viewed 13 September 2022]. Available from: <https://www.theverge.com/2021/10/4/22709575/facebook-outage-instagram-whatsapp>

HOLT, K., 2019. Facebook Fined Yet Again Over Cambridge Analytica Scandal. Forbes, 30 Dec

JAMES, L., 2022. Global chip shortage 2022 – updates in April [viewed 8 June 2022]. Available from: <https://www.power-and-beyond.com/global-chip-shortage-2022-updates-in-april-a-d01d7c355faee7f829a50d99c4fa8e85/>

JULIA CARRIE WONG, 2019. The Cambridge Analytica scandal changed the world – but it didn’t change Facebook [viewed 7 June 2022]. Available from: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>

KEAR, S., 2011. Introduction to pfSense-An Open Source Firewall and Router Platform [viewed 15 July 2022]. Available from: <https://turbofuture.com/computers/Introduction-to-pfSense-An-Open-Source-Firewall-and-Router-Platform>

KRATKY-KATZ, M., 2021. 2021 PageFair Adblock Report - Blockthrough [viewed 10 September 2022]. Available from: <https://blockthrough.com/blog/2021-adblock-report>

LawInsider., 2022. Unforeseen Circumstances Sample Clauses: 200 Samples | Law Insider [viewed 21 September 2022]. Available from: <https://www.lawinsider.com/clause/unforeseen-circumstances>

LAYTON, R., 2022. Crypto Hacking And Power Outages: Buyers Beware On AWS Cloud. Forbes, 24 Jan

Linden, E., 2022. Killed by Apple, Google and Microsoft - Discontinued products and services [viewed 13 September 2022]. Available from: <https://killedby.tech/>

LOMAS, N., 2022. EU's new rules for Big Tech to come into force next Spring [viewed 21 September 2022]. Available from: <https://techcrunch.com/2022/05/05/digital-markets-act-enforcement-margrethe-vestager/>

LUMLEY-SAVILE, P., 2012. Force majeure and cloud computing contracts [viewed 22 September 2022]. Available from: <https://www.lexology.com/commentary/tech-data-telecoms-media/united-kingdom/rpc/force-majeure-and-cloud-computing-contracts>

McGuire, L., 2020. What Is Digital Agility? | Formstack Blog [viewed 21 September 2022]. Available from: <https://www.formstack.com/resources/blog-what-is-digital-agility>

MILLWARD W, 2022. Microsoft Azure DevOps Targeted By Hacker Group: Reports [viewed 9 June 2022]. Available from: <https://www.crn.com/news/security/microsoft-azure-devops-targeted-by-hacker-group-reports>

MUHAMMAD, Z., 2022. The Big Five Tech Companies (Apple, Amazon, Alphabet, Microsoft and Meta) Earned Over \$1.4 Trillion Last Year, Here's Where That Money Came From [viewed 5 June 2022]. Available from: <https://www.digitalinformationworld.com/2022/05/the-big-five-tech-companies-apple.html>

National Grid., 2017. Black Start Strategy Black Start Strategy. Available from: <https://www.nationalgrid.com/sites/default/files/documents/High%20Level%20Black%20Start%20Strategy.pdf>

Netgate., 2022. Packages — pfBlocker-NG Package | pfSense Documentation [viewed 15 September 2022]. Available from: <https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html>

Nevard, E., 2021. Whistleblower: Ubiquiti Breach 'Catastrophic' [viewed 9 June 2022]. Available from: <https://blog.thisisanitsupportgroup.com/whistleblower-ubiquiti-breach-catastrophic/>

O'Donnell, J., 2020. Does Your Organization Need Cloud Visibility? | CloudBolt Software [viewed 9 June 2022]. Available from: <https://www.cloudbolt.io/blog/does-your-organization-need-cloud-visibility>

Ovide, S., 2021. Big Tech Has Outgrown This Planet. The New York Times

PÉREZ DE LAMO, D., 2021. The Hague -Seminar for Young Academics and Practitioners [viewed 22 September 2022]. Available from: <https://fide2020.eu/wp-content/uploads/2021/12/III-1-David-Peerez-de-Lamo-FIDE-2021-Killer-Acquisitions1.pdf>

Philip., C., 2022. Government sets out plans for how tech regulator will tackle dominance of major firms [viewed 21 September 2022]. Available from: <https://www.gov.uk/government/news/government-sets-out-plans-for-how-tech-regulator-will-tackle-dominance-of-major-firms>

PI-HOLE, 2022. Pi-hole/pi-hole: A black hole for Internet advertisements [viewed 14 September 2022]. Available from: <https://github.com/pi-hole/pi-hole>

PM2., 2022. PM2 - Home [viewed 20 September 2022]. Available from: <https://pm2.keymetrics.io/>

Pollina E., Quaglia M., 2021. Italy fines Amazon record \$1.3 bln for abuse of market dominance [viewed 11 September 2022]. Available from: <https://www.reuters.com/technology/italys-antitrust-fines-amazon-113-bln-euros-alleged-abuse-market-dominance-2021-12-09/>



RAČKAUSKAS, E., 2021. What Is ICANN – The Internet Corporation for Assigned Names and Numbers? [viewed 11 September 2022]. Available from: <https://www.ipxo.com/blog/what-is-icann>

Reduce Reuse Recycle., 2022. Reduce Reuse Recycle [viewed 15 September 2022]. Available from: <https://www.reducereuserecycle.co.uk/>

REUTERS, 2021., Amazon hit with record EU data privacy fine [viewed 11 September 2022]. Available from: <https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/>

RUTKIN, A. et al., 2020. Investigation of Competition in Digital Markets Available from: [https://judiciary.house.gov/uploadedfiles/competition\\_in\\_digital\\_markets.pdf](https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf)

SALMELA, J., 2015. Block Millions Of Ads Network-wide With A Raspberry Pi-hole 2.0 [viewed 14 September 2022]. Available from: <https://jacobsalmela.com/2015/06/16/block-millions-ads-network-wide-with-a-raspberry-pi-hole-2-0/>

SEIBT, S., 2022. *Ukraine conflict presents a minefield for Anonymous and hacktivists* [viewed 15 July 2022]. Available from: <https://www.france24.com/en/europe/20220323-ukraine-conflict-presents-a-minefield-for-anonymous-and-hacktivists>

SEVILLA, G., 2022. Ireland’s privacy watchdog fines Meta \$400M for mishandling children’s user data [viewed 11 September 2022]. Available from: <https://www.insiderintelligence.com/content/ireland-s-privacy-watchdog-fines-meta-400m-mishandling-children-s-user-data>

Singleton, S., 2000. How Cookie-Gate Crumbles [viewed 14 September 2022]. Available from: <https://www.cato.org/commentary/how-cookie-gate-crumbles>

SLAGER, D., 2021. Council Post: In The Cookieless Future, Big Tech Stands To Gain The Most. Forbes, 21 Apr

Spanning., 2013. Top Threats to Cloud Computing #4: Lack of Due Diligence | Spanning [viewed 9 June 2022]. Available from: <https://spanning.com/blog/top-threats-to-cloud-computing-4-lack-of-due-diligence/>

Stancil, K., 2022. Big Tech ‘Fundamentally At Odds With Children’s Well-Being,’ Advocates Say [viewed 11 September 2022]. Available from: <https://www.commondreams.org/news/2022/03/22/big-tech-fundamentally-odds-childrens-well-being-advocates-say>

SUTRICH, N., 2021. The AWS outage that took down Ring, Alexa, and Disney+ is finally over [viewed 9 June 2022]. Available from: <https://www.androidcentral.com/ring-and-parts-aws-are-down-right-now>

SYAL, R., 2021. Priti Patel pressed to explain award of spy agencies cloud contract to Amazon [viewed 9 June 2022]. Available from: <https://www.theguardian.com/uk-news/2021/oct/26/amazon-web-services-aws-contract-data-mi5-mi6-gchq>

The Verge., 2018. Zuckerberg’s EU testimony: what he didn’t answer. YouTube

TODOROV, G., 2022. 10+ Essential CDN Stats about Internet Traffic and Usage [viewed 13 July 2022]. Available from: <https://thrivemyway.com/cdn-stats/>

TOWNSEND, M., 2022. Facebook-Cambridge Analytica data breach lawsuit ends in 11th hour settlement [viewed 11 September 2022]. Available from: <https://www.theguardian.com/technology/2022/aug/27/facebook-cambridge-analytica-data-breach-lawsuit-ends-in-11th-hour-settlement>

Tozzi, C., 2021. Is Amazon's Cloud Control Like Microsoft's Monopoly of the OS? [viewed 8 June 2022]. Available from: <https://www.itprotoday.com/iaaspaas/amazons-cloud-control-microsoft-s-monopoly-os>

UK Government., 2021. CMA fines Facebook over enforcement order breach [viewed 11 September 2022]. Available from: <https://www.gov.uk/government/news/cma-fines-facebook-over-enforcement-order-breach>

WATERS, R., 2020. Big Tech's 'buy and kill' tactics come under scrutiny [viewed 6 June 2022]. Available from: <https://www.ft.com/content/39b5c3a8-4e1a-11ea-95a0-43d18ec715f5>

WILHELM, A., 2021. Big Tech is now worth so much we've forgotten to be shocked by the numbers [viewed 5 June 2022]. Available from: <https://techcrunch.com/2021/05/01/big-tech-is-now-worth-so-much-weve-forgotten-to-be-shocked-by-the-numbers>

Williams, L., 2020. TCP/IP Model: What are Layers & Protocol? TCP/IP Stack [viewed 15 September 2022]. Available from: <https://www.guru99.com/tcp-ip-model.html>

WILLIAMS, M., 2022. The best VPN service 2022 [viewed 19 September 2022]. Available from: <https://www.techradar.com/vpn/best-vpn>

Windows 11 criticized for being an internet-reliant OS - You Have to Sign in to a Microsoft Account to Use Windows 11 THOMAS, J., 2022. Windows 11 will soon be closed off to anyone without internet [viewed 14 September 2022]. Available from: <https://www.techradar.com/news/upcoming-windows-11-pro-update-will-force-you-to-have-an-internet-connection>

WNIP, 2021. The ending of third-party cookies: Big tech developments | What's New in Publishing | Digital Publishing News [viewed 15 September 2022]. Available from: <https://whatsnewinpublishing.com/the-ending-of-third-party-cookies-big-tech-developments/>

worldometer., 2017. GDP by Country - Worldometer [viewed 5 June 2022]. Available from: <https://www.worldometers.info/gdp/gdp-by-country/>

## 10. Appendix A – Letters to Organisations

### DUCKDUCKGO

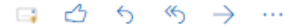
Regarding DuckDuckGo's Dependency on Microsoft



Edward Nevard

Wed 21/09/2022 11:36

To: open@duckduckgo.com; press@duckduckgo.com



To whom this may concern,

I was recently conducting an experiment as a component of my master's thesis whereby I assess the effects of Big Tech dependency by preventing devices on the network from accessing any of their network at Layer 3, by ASN IP addresses at the network edge-firewall.

The participants and I in the study were surprised to find that DuckDuckGo uses Microsoft services to host the platform, rendering it an unavailable search engine for those who made the ethical decision not to use Big Tech services (which includes Microsoft).

Many the participants referenced DuckDuckGo as a great search engine alternative and were positive about DuckDuckGo as an organisation but were disappointed to find that it is not accessible because its backend uses Microsoft after finding your website IP addresses are in the Microsoft ASN.

My main questions are:

- 1) Why do you use Microsoft services to host your platform whilst boasting about privacy protection, and how do you ensure all your visitor's information (IP address, client type, etc) is kept safe despite travelling through their network?
- 2) Do you have any plans to move away Microsoft Corporation for hosting your search engine platform in any capacity?

Thank you so much for your time, I would really appreciate a comment ahead of my study being published.

Kind regards,

Ed

**Ed Nevard**

Student Course Rep | MSc Cyber Security Engineering  
Faculty of Business, Law & Digital Technologies

**SOLENT**  
UNIVERSITY

East Park Terrace  
Southampton SO14 0YN  
[www.solent.ac.uk](http://www.solent.ac.uk)

SOLENT  
STUDENTS'  
UNION

NUS  
Quality  
Students'  
Union

STARS  
LEVEL 4  
ACHIEVEMENT

National Centre for Diversity  
75% 190 2019

MINDFUL  
EMPLOYER

Solent Students' Union is a not-for-profit organisation, all revenue generated is re-invested back in to services for our students.

[www.solent.ac.uk](http://www.solent.ac.uk) 0238 201 3388 Charity Number: 1153350

As part of our Green Impact promise we are asking staff, students and external visitors to try and use sustainable transport where they can.  
Could you walk, cycle or use public transport to get to your next meeting?

Make your own green impact & don't print this email.

Let's connect!

[Reply](#) | [Reply all](#) | [Forward](#)

Figure 39: Email to DuckDuckGo

*I did not receive a response from DuckDuckGo to date.*

## SECRETARY OF STATE FOR EDUCATION

Edward Charles Nevard

Hampshire, SO31 5  
4nevae40@solent.ac.uk  
5th September 2022

The Rt Hon James Cleverly MP, Secretary of State for Education  
House of Commons  
London, SW1A 0AA  
james.cleverly.mp@parliament.uk

Dear The Rt Hon James Cleverly MP,

I am writing to you today to ask a series of questions regarding the national curriculum in the UK for primary & secondary schools which concern the Information Technology and Computing subject(s).

I am in the process of writing my dissertation for my MSc Cyber Security Engineering degree at Southampton Solent University. One of the sections within this is focuses on both the education of our current and future young people on civil cyber security and data awareness online.

Our current curriculum for Information Technology within schools very much still focuses on user skills and remains very similar to when I started secondary school in 2011, though the general landscape of the internet has transformed dramatically within this time. The European Union are beginning to act accordingly with the introduction of new legislation in recent years, and the current proposed Digital Markets Act.

My main question to you is, are there any current plans to implement civil cyber security and digital self-defence within the national curriculum for school pupils?

This is a unique matter, in the sense that these issues and concerns simply did not exist for previous generations, and therefore many parents are not educated and/or aware enough to keep their children and their children's data protected online. Therefore, our schools have a stronger responsibility to teach and convey the importance of online safety and personal data protection.

In addition to this, do you believe the UK Government are aware of the increasing risks surrounding data security online and the Big Technology companies (Amazon, Apple, Google, Meta (Facebook) & Microsoft) collecting and using data on millions of our citizens including children without being properly regulated?

Thank you in advance for your time, I very much look forward to your response.

Yours faithfully,

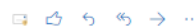
*E Nevard*

Edward Charles Nevard BSc (Hons)

*Figure 40: Email to Secretary of State for Education*



ACCOUNT, Unmonitored <Unmonitored.ACCOUNT@education.gov.uk>  
Thu 22/09/2022 12:14  
To: Edward Nevard



Dear Mr Nevard

I am writing to thank you for your letter of 5 September addressed to the former Secretary of State about implementing civil cyber security and digital self-defence learning within the national curriculum for school pupils. Your letter has been passed to me and I have been asked to reply.

The government is committed to ensuring that all pupils are taught about e-safety. The computing curriculum, introduced in September 2014, took positive action by including e-safety content throughout all of the key stages. From key stage one pupils are taught how to use technology safely and respectfully, to keep personal information private and where to go for help and support when they have concerns about the content they find or the contact they receive from others.

The curriculum responds to the different and escalating risks that young people face as they become older, with flexibility built into its programmes of study to enable schools to choose how they teach their children about the dangers of social media in an age-appropriate way.

To support teachers in teaching the computing curriculum, the Department for Education funded National Centre for Computing Education (NCCE) launched in November 2018, providing professional development and teaching resources to support teachers of computing.

As part of their work on e-safety, the NCCE have:

- published free online teaching resources covering e-safety topics on their 'Teach Computing Curriculum' website;
- worked with the UK Safer Internet Centre to produce a key stage 4 'Computing for All' course which covers ways of teaching e-safety as part of a wider approach;
- created a GCSE-Level 'Introduction to Cybersecurity' course which focuses on the range of threats and vulnerabilities that exist on the internet, how they could be exploited and how to mitigate against cyber-attacks; and
- worked with the National Crime Agency, and the National Cyber Security Centre to share expertise and signpost to resources such as the CyberFirst programme.

It should be noted that the computing curriculum is very different from the previous subject of ICT. The computing curriculum has a focus on ensuring that all pupils can understand and apply the fundamental principles and concepts of computer science, and that they can analyse problems in computational terms. It ensures that pupils have practical experience of writing computer programs, that they can evaluate and apply information technology, and are responsible, competent, confident and creative users of information and communication technology. The computing curriculum is available online and can be found on GOV.UK. It is mandatory in all state-maintained schools, and free schools and academies may use it as an exemplar.

With specific regard to online safety, most children have a positive experience online, using the internet for connecting with peers, as well as to access educational resources, information, and entertainment. However, the impact of harmful content and activity online can be particularly damaging for children and there are growing concerns about the potential impact on their mental health and wellbeing. The Online Safety Bill will make the UK the safest place to be a child online and the strongest protections in this framework are for children. The Bill, introduced to parliament on 17 March 2022, is currently in report stage in the House of Commons and can be viewed at the following link: <https://bills.parliament.uk/bills/3137/publications>

All companies in scope of the legislation will have to do far more to address illegal content and activity on their service and, where they are likely to be accessed by children, put in place safety measures to protect them from harmful content like pornography, and behaviour such as bullying. Ofcom will be able to take enforcement action, including large fines, against companies that fail to comply with these duties.

Ahead of online safety legislation, the Information Commissioner's Age Appropriate Design Code came into force in September 2021. This provides stronger protections for children's personal data and guidance to companies on the privacy standards they must adopt when they are offering online services and applications that children are likely to access and which process their personal data. Services in scope of the Code, which include social media platforms, need to make sure that they consider children when designing their sites and protect them adequately.

Furthermore, as part of the National Cyber Strategy, there are a number of extra-curricular initiatives aimed at young people which aim to build their enthusiasm, awareness and learning of cyber security. This includes the 'Cyber Explorers' programme, run by the Department for Digital, Culture, Media and Sport, that reached over 23,000 young people aged 11 - 14 in the last six months: <https://www.cyberexplorers.co.uk/>

The government's National Cyber Security Centre also offers a range of interactive cyber security resources for young people, including the 'Cyber Sprinters' game for 7 to 11 year olds: <https://www.ncsc.gov.uk/collection/cybersprinters>

More information on the National Cyber Strategy is available here: <https://www.gov.uk/government/publications/national-cyber-strategy-2022>  
I hope this information is useful to you.

Thank you once again for taking the time to write to the department.

Your correspondence has been allocated reference number 2022-0033658. If you need to respond to us, please visit <https://www.education.gov.uk/contactus> and quote your reference number.

As part of our commitment to improving the service we provide to our customers, we are interested in hearing your views and would welcome your comments via our website at: <https://form.education.gov.uk/service/TOCMFeedback>

Yours sincerely

A Townsend  
Ministerial and Public Communications Division  
Web: <https://www.education.gov.uk>  
Twitter: <https://www.twitter.com/educationgovuk>  
Facebook: <https://www.facebook.com/educationgovuk>



Department  
for Education

**Figure 41: Reply from Department for Education**

## 11. Appendix B – Big Tech Acquisitions

Data Acquired from the American Economic Liberties Project & sorted into tables (American Economic Liberties Project, 2022).

### AMAZON

118 acquisitions over 25 years or ~5 deals per year.

Date	Company
March 2022	Strio.AI
April 2022	GlowRoad
January 2021	Umbr3 3D
February 2021	Selz
June 2021	Art19 and Wickr
November 2021	Veeqo
June 2020	Zoox
January 2019	CloudEndure and TSO Logic
February 2019	Eero and Dispatch AI
April 2019	CANVAS Technology
May 2019	Sizmek Ad Server
June 2019	Bebo
July 2019	E8 Storage
September 2019	IGDB and INLT
October 2019	Health Navigator
January 2018	Sqrrl
February 2018	Immedia
April 2018	Ring
June 2018	PillPack
August 2018	Tapzo
January 2017	harvest.ai
February 2017	Colis Privé
March 2017	Do.com and Thinkbox Systems
June 2017	Whole Foods
July 2017	Graphiq, GameSparks and Souq.com
September 2017	Wing
October 2017	Body Labs
November 2017	Goo Technologies
December 2017	Blink
February 2016	NICE and Emvantage Payments
April 2016	Orbeus
July 2016	Cloud9 IDE
August 2016	Curse Inc.
October 2016	Westland
November 2016	Biba Systems and Partpic
January 2015	Annapurna Labs
March 2015	2lemetry
April 2015	Shoefitr, ClusterK and Amiato
July 2015	AppThwack
September 2015	Elemental Technologies and Safaba Translation Systems
February 2014	Double Helix Games

<b>April 2014</b>	ComiXology
<b>August 2014</b>	Twitch Interactive
<b>October 2014</b>	Rooftop Media
<b>December 2014</b>	GoodGame
<b>January 2013</b>	INOVA Software
<b>March 2013</b>	Goodreads
<b>May 2013</b>	Liquavista
<b>October 2013</b>	TenMarks Education
<b>February 2012</b>	Teachstreet
<b>March 2012</b>	Kiva Systems
<b>April 2012</b>	Evi and Avalon Books
<b>July 2012</b>	UpNext
<b>July 2011</b>	Pushbutton and bookdepository.com
<b>September 2011</b>	Yap
<b>February 2010</b>	Touchco
<b>June 2010</b>	woot.com
<b>September 2010</b>	Amie Street
<b>October 2010</b>	BuyVIP
<b>November 2010</b>	Toby Press, Quidsi, Soap.com, Diapers.com, BeautyBar.com and Wag.com
<b>April 2009</b>	Lexcycle
<b>June 2009</b>	SnapTell
<b>July 2009</b>	Zappos.com
<b>January 2008</b>	Without A Box and Audible
<b>April 2008</b>	LOVEFiLM
<b>June 2008</b>	Fabric.com
<b>July 2008</b>	Box Office Mojo
<b>August 2008</b>	Shelfari
<b>October 2008</b>	Reflexive Entertainment
<b>December 2008</b>	AbeBooks and bookfinder.com
<b>May 2007</b>	BrillianceAudio and Digital Photography Review
<b>February 2006</b>	EastDane and Shopbop.com
<b>October 2006</b>	Text Pay Me
<b>April 2005</b>	MobiPocket and BookSurge
<b>June 2005</b>	Small Parts Inc
<b>July 2005</b>	CustomFlix
<b>August 2004</b>	Joyo.com
<b>January 2002</b>	Egghead.com
<b>December 2001</b>	OurHouse
<b>January 1999</b>	MindCorps
<b>April 1999</b>	e-Niche Inc.
<b>1998</b>	PlanetAll.com, Jungle, Bookpages, Telebook, and IMDb

*Table 6: Big Tech Acquisitions - Amazon*

## APPLE

126 acquisitions over 34 years or ~4 deals per year

Date	Company
January 2021	Curious AI
August 2021	Primephonic
January 2020	Xnor.ai
March 2020	DarkSky
April 2020	Voysis
May 2020	NextVR and Inductiv
June 2020	Fleetsmith
July 2020	Mobeewave
August 2020	Camerei and Spaces
February 2019	DataTiger and PullString
March 2019	Laserlike and Stamplay
May 2019	Tueo Health
June 2019	Drive.ai
July 2019	Intel's smartphone modem business
October 2019	Ikinema
December 2019	Spectral Edge
January 2018	Silicon Valley Data Science and Buddybuild
March 2018	Texture
August 2018	Akonia Holographics
September 2018	Shazam
October 2018	Dialog
November 2018	Silk Labs
December 2018	Platoon
February 2017	RealFace
March 2017	Workflow
May 2017	Beddit and Lattice Data
June 2017	SensoMotoric Instruments
September 2017	Regaind
October 2017	init.ai and PowerbyProxi
November 2017	InVisage Technologies and Vrvana
December 2017	Pop Up Archive and Spektral
January 2016	Emotient, LearnSprout and Flyby Media
August 2016	Turi and Glimpse
September 2016	tuplejump
December 2016	Indoor.io
January 2015	Musicmetric and Semetric
February 2015	Camel Audio
March 2015	FoundationDB
April 2015	LinX and Dryft
May 2015	Coherent Navigation and Metaio
September 2015	Mapsense
October 2015	Vocal IQ and Perceptio
November 2015	Faceshift and LegbaCore
January 2014	SnappyLabs
February 2014	Burstly and TestFlight App



<b>May 2014</b>	LuxVue Technologies
<b>June 2014</b>	Spotsetter and Swell
<b>July 2014</b>	BookLamp
<b>August 2014</b>	Beats Electronics
<b>September 2014</b>	Prss
<b>January 2013</b>	Novauris Technologies
<b>March 2013</b>	WiFiSlam
<b>June 2013</b>	Ottocat
<b>July 2013</b>	Catch.com, Locationary and HopStop.com
<b>August 2013</b>	Passif Semiconductor, Matcha, Embark and AlgoTrim
<b>October 2013</b>	Cue
<b>November 2013</b>	PrimeSense
<b>December 2013</b>	Acunu, Topsy and BroadMap
<b>2012</b>	Anobit, Chomp, AuthenTec, Particle and Redmatica
<b>2011</b>	C3 Technologies
<b>2010</b>	Quattro Wireless, Intrinsicity, Siri, Gypsy Moth Studios, Poly9, Polar Rose and IMSense
<b>2009</b>	Placebase and Lala
<b>2008</b>	P.A. Semi
<b>2006</b>	Silicon Color and Proximity
<b>2005</b>	SchemaSoft and FingerWorks
<b>2002</b>	Nothing Real, Zayante, Silicon Grail Corp-Chalice, Propel Software, Prismo Graphics and Emagic
<b>2001</b>	Bluefish Labs, bluebuzz, Spruce Technologies and PowerSchool
<b>2000</b>	NetSelector, Astarte-DVD Authoring Software, and SoundJam MP
<b>1999</b>	Xemplar Education and Raycer Graphics
<b>1997</b>	Next and Power Computing Corp
<b>1989</b>	Coral Software
<b>1988</b>	Network Innovations, Orion Network Systems, Styleware, and Nashoba Systems

*Table 7: Big Tech Acquisitions - Apple*

## FACEBOOK (META)

92 acquisitions over 17 years or ~6 deals per year

<b>Date</b>	<b>Company</b>
October 2021	AI.Reverie and Within
June 2021	Unit 2 Games and BigBox VR
April 2021	Downpour Interactive
November 2020	Kustomer
June 2020	Mapillary and Ready at Dawn
February 2020	PlayGiga and Sanzaru Games
December 2019	Beat Games
November 2019	Packagd
September 2019	GrokStyle, Servicefriend, and CTRL-labs
February 2019	Vidpresso and Chainspace
August 2018	Redkix
July 2018	confirm.io and Bloomsbury AI
January 2018	tbh
October 2017	Fayteq
August 2017	Source3
July 2017	Zurich Eye and Ozlo
November 2016	InfiniLED, CrowdTangle, and FacioMetrics
October 2016	Nascent Objects
September 2016	Two Big Ears
May 2016	Masquerade
March 2016	Endaga
October 2015	Pebbles Interfaces
July 2015	Surreal Vision
May 2015	TheFind
March 2015	QuickFire
January 2015	Wave Group Sound and wit.ai
August 2014	PRYTE, privatecore, and LiveRail
June 2014	ProtoGeo Oy
April 2014	Ascenta
March 2014	WhatsApp and Oculus VR
February 2014	Branch
January 2014	SportStream and Little Eye Labs
December 2013	Onavo
October 2013	Jibbigo
August 2013	Monoidics
July 2013	Parse
April 2013	Hot Studio and Spaceport
March 2013	Atlas Solutions, Osmeta, and Storylane
February 2013	threadsy
July 2012	Spool and Acrylic Software
June 2012	face.com
May 2012	Karma, Gancee and Lightbox.com
April 2012	TagTile and Instagram
December 2011	Gowalla
November 2011	Strobe

<b>October 2011</b>	friend.ly
<b>August 2011</b>	Push Pop Press
<b>June 2011</b>	MailRank and Sofa
<b>April 2011</b>	DayTum
<b>March 2011</b>	RecRec, Beluga, and Snaptu
<b>January 2011</b>	Rel8tion
<b>November 2010</b>	Zenbe
<b>November 2010</b>	FB.com domain name
<b>October 2010</b>	drop.io
<b>August 2010</b>	Hot Potato and Chai Labs
<b>July 2010</b>	nextstop
<b>May 2010</b>	ShareGrove and friendster
<b>March 2010</b>	Divvyshot
<b>February 2010</b>	Octazen
<b>August 2009</b>	FriendFeed
<b>June 2008</b>	ConnectU
<b>July 2007</b>	Parakey
<b>August 2005</b>	aboutface

*Table 8: Big Tech Acquisitions – Facebook (Meta)*

## GOOGLE

264 acquisitions over 21 years or 13 deals per year.

<b>February 2001</b>	<b>Deja</b>
<b>May 2022</b>	Raxium
<b>April 2022</b>	MobiledgeX and Vicarious
<b>January 2022</b>	Siemplify
<b>October 2021</b>	MuJoCo
<b>September 2021</b>	Playspace
<b>April 2021</b>	Dysonics
<b>February 2021</b>	Provino
<b>January 2021</b>	Fitbit
<b>December 2020</b>	Actifio
<b>August 2020</b>	StratoZone
<b>June 2020</b>	North
<b>February 2020</b>	Looker and Cornerstone Technology
<b>January 2020</b>	AppSheet and Pointy
<b>December 2019</b>	Typhoon Studios
<b>November 2019</b>	CloudSimple
<b>August 2019</b>	Socratic
<b>July 2019</b>	Elastifile
<b>March 2019</b>	Nightcorn
<b>February 2019</b>	Alooma
<b>January 2019</b>	Superpod
<b>December 2018</b>	Where is My Train and Sigmoid Labs
<b>November 2018</b>	Workbench
<b>October 2018</b>	Onward
<b>August 2018</b>	GraphicsFuzz
<b>May 2018</b>	Velostrata and Cask

<b>March 2018</b>	Lytro and Tenor
<b>February 2018</b>	Xively
<b>January 2018</b>	Limes Audio, Redux and HTC Corporation
<b>November 2017</b>	Banter
<b>October 2017</b>	Relay Media and 60db
<b>September 2017</b>	Bitium
<b>August 2017</b>	AlMatter and Senosis
<b>July 2017</b>	Halli Labs
<b>May 2017</b>	Owlchemy Labs
<b>March 2017</b>	Kaggle and AppBridge
<b>January 2017</b>	Crashlytics and Fabric
<b>December 2016</b>	Cronologics
<b>November 2016</b>	LeapDroid and Qwiklabs
<b>October 2016</b>	FameBit and Eyefluence
<b>September 2016</b>	Apigee, Urban Engines and Api.ai
<b>August 2016</b>	Orbitera and Apportable
<b>July 2016</b>	Moodstocks, Anvato, Kifi and LaunchKit
<b>June 2016</b>	Webpass
<b>May 2016</b>	Synergise
<b>February 2016</b>	BandPage and Pie
<b>November 2015</b>	Fly Labs and Bebop
<b>October 2015</b>	Digisfera
<b>September 2015</b>	Oyster and Jibe Mobile
<b>July 2015</b>	Pixate
<b>May 2015</b>	Timeful and Pulse.io
<b>April 2015</b>	Thrive Audio and Skillman & Hackett
<b>February 2015</b>	Launchpad Toys, Odysee, Softcard and Red Hot Labs
<b>January 2015</b>	Granata Decision Systems
<b>December 2014</b>	Vidmaker
<b>November 2014</b>	Lumedyne Technologies and RelativeWave
<b>October 2014</b>	Agawi, Firebase, Dark Blue Labs, Vision Factory and Revolv
<b>September 2014</b>	Lift Labs, Polar and Input Factory
<b>August 2014</b>	Skybox Imaging, Emu, Directr, Jetpac, Gecko Design, and Zync Render
<b>July 2014</b>	Dropcam, Songza and drawElements
<b>June 2014</b>	mDialog, Aplental Technologies, Baarzo, and Appurify
<b>May 2014</b>	Rangespan, Adometry, Appetas, Stackdriver, Quest Visual, Gridcentric and Divide
<b>April 2014</b>	Titan Aerospace
<b>March 2014</b>	GreenThrottle
<b>February 2014</b>	Nest, SlickLogin and spider.io
<b>January 2014</b>	Bitspin, Imprerium and DeepMind Technologies
<b>October 2013</b>	Flutter and FlexyCore
<b>September 2013</b>	Calico and Bump
<b>August 2013</b>	WIMM Labs
<b>June 2013</b>	Waze

<b>May 2013</b>	Makani Power and MyEnergy (SHUT DOWN)
<b>April 2013</b>	Behavio and Wavii
<b>March 2013</b>	Channel Intelligence, DNNresearch, and Talaria Technologies
<b>January 2013</b>	Schaft, Industrial Preception, Redwood Robotics, Meka Robotics, Holomni, Bot & Dolly, and Autofuss
<b>November 2012</b>	Incentive Targeting and Bufferbox
<b>September 2012</b>	VirusTotal.com and Nik Software
<b>July 2012</b>	Sparrow, Wildfire Interactive and Cuban Council
<b>June 2012</b>	Meebo and Quickoffice
<b>April 2012</b>	TxVia
<b>March 2012</b>	Milk
<b>December 2011</b>	RightsFlow and Clever Sense
<b>November 2011</b>	Apture and Katango
<b>October 2011</b>	Anthony's Robots, SocialGrapple and 510 Systems
<b>September 2011</b>	Zave Networks, Zagat and DailyDeal
<b>August 2011</b>	Dealmap and Motorola Mobility (SOLD 2013)
<b>July 2011</b>	Punchd, Fridge and PittPatt
<b>June 2011</b>	PostRank, Admeld, and Sage TV
<b>May 2011</b>	Modu and Sparkbuy
<b>April 2011</b>	PushLife, ITA Software and TalkBin
<b>March 2011</b>	BeatThatQuote.com, Next New Networks, Green Parrot Pictures and Zynamics
<b>January 2011</b>	eBook Technologies and SayNow
<b>December 2010</b>	Phonetic Arts, Widevine Technologies and Zetawire
<b>October 2010</b>	BlindType
<b>September 2010</b>	Plannr, Quiksee and MentorWave Technologies
<b>August 2010</b>	Slide.com, Jambool, Like.com, Angstro and SocialDeck
<b>July 2010</b>	Metaweb
<b>June 2010</b>	Invite Media and Instantiations
<b>May 2010</b>	Global IP Solutions, Simplify Media and Ruba.com
<b>April 2010</b>	PinkArt, Agnilux, LabPixies and BumpTop
<b>March 2010</b>	Picnik, DocVerse and Episodic
<b>February 2010</b>	Aardvark
<b>February 2010</b>	reMail
<b>November 2009</b>	AdMob, Gizmo5, Teracent and AppJet
<b>September 2009</b>	reCAPTCHA
<b>August 2009</b>	On2
<b>April 2009</b>	Eluceon Research
<b>September 2008</b>	TNC
<b>July 2008</b>	Begun and Omnisio
<b>October 2007</b>	Jaiku
<b>September 2007</b>	Zingku
<b>July 2007</b>	Postini and ImageAmerica
<b>June 2007</b>	FeedBurner, PeaksStream, Zenter and GrandCentral
<b>May 2007</b>	GreenBorder and Panoramio

<b>April 2007</b>	DoubleClick, Tonic Systems and Marratech video conference software
<b>March 2007</b>	Trendalyzer
<b>February 2007</b>	AdScape
<b>December 2006</b>	Endoxon
<b>October 2006</b>	JotSpot and Youtube
<b>August 2006</b>	Neven Vision
<b>June 2006</b>	2Web Technologies
<b>April 2006</b>	Orion
<b>March 2006</b>	Upstartle and “@” Last Software
<b>February 2006</b>	Measure Map
<b>January 2006</b>	dMarc Broadcasting
<b>December 2005</b>	Phatbits, allPAY GmbH and bruNET GmbH
<b>November 2005</b>	Skia and Akwan Information Technologies
<b>August 2005</b>	Android
<b>July 2005</b>	Reqwireless
<b>May 2005</b>	Dodgeball
<b>March 2005</b>	Urchin Software Corp
<b>October 2004</b>	Where 2 Technologies and Keyhole
<b>September 2004</b>	ZipDash
<b>July 2004</b>	Picasa
<b>May 2004</b>	Ignite Logic
<b>October 2003</b>	Sprinks and Genius Labs
<b>April 2003</b>	Neotonic Software, Applied Semantics and Kaltix
<b>February 2003</b>	Pyra Labs
<b>September 2001</b>	Outride

*Table 9: Big Tech Acquisitions - Google*