5-2021

PRIVACY IS INFRINGED IN PLAIN SIGHT AND HOW TO DISSAPEAR

Zachary Taylor

PRIVACY IS INFRINGED IN PLAIN SIGHT AND HOW TO DISAPEAR

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

---

by

Zachary P. Taylor

May 2021

PRIVACY IS INFRINGED IN PLAIN SIGHT AND HOW TO DISSAPEAR

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Zachary P. Taylor

May 2021

Approved by:

Vincent Nestler PhD, Committee Member, Project Chair

Conrad Shayo PhD, Committee Member, Reader

Javad Varzandeh PhD, Committee Member, IDS Department Chair

ABSTRACT

This culminating project explored how Amazon, Apple, Facebook, Google, and Microsoft infringe on their user's information privacy. Focus was on tools and techniques one can use to strengthen their information privacy. Privacy or information privacy was defined as the right to have some control over how your personal information is collected and used. This project will also introduce a verity of open-source tools and techniques that would help the unsuspected user to maintain their privacy.The questions asked were: what are some common techniques that Amazon, Apple, Facebook, Google, or Microsoft use to gain personal information?, At what cost would it take for someone to maintain their privacy online without interacting with Amazon, Apple, Facebook, Google, or Microsoft ?, What are some reasonable recommendations would I recommend to the average unsuspecting user ? The project findings were: that major technology companies make money from intruding on their user’s privacy, and that the upkeep cost for one to maintain their privacy can be expensive, and that it will be difficult for one to maintain their privacy overtime. Some of the recommendations for further suggested research include: cell phones, faraday bags, and Redundancy.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:

INTRODUCTION

People in the 21st century seem to want to connect everything to the internet, hence the term Internet of Things (IoT). However, people need to be aware that they have invited a privacy intruder to their place of residency and that the companies behind those applications and devices will do anything in their power to intrude the privacy of their unsuspecting customers at any cost. Privacy Policy, tracking cookies, and freeware are major threats to the customer user's privacy. This project will mainly focus on (1) how Amazon, Apple, Facebook, Google, and Microsoft infringe on their user's information privacy and (2) some of the tools and techniques a customer user can use to strengthen their information privacy.

The International Association of Privacy Professionals' website defines Privacy or information privacy "as the right to have some control over how your personal information is collected and used"(IAAP). Some types of user information include, device information, personal identifiable information (PII), and browsing activity. Information that a user provides when using a product or service from one of the five major technology companies can expose their device identification, location, and even their identity; all of the information being collected and analyzed through the technology companies' advertising network. This is why it is important to provide knowledge to people on what type of

information is being collected about them, how these companies are able to do so, and what they can do about it. This begs three questions:

1. What are some common techniques that Amazon, Apple, Microsoft, Facebook, or Google use to gain personal information?
2. At what cost would it take for someone to maintain their privacy online without interacting with Amazon, Apple, Microsoft, Facebook, or Google?
3. What are some reasonable recommendations would I recommend to the average unsuspecting user?

This project will explain information privacy, how it is commonly exploited, tools and techniques used to defend information from being exposed. This project will go over laws and regulations currently in place that pertain to the use of protecting one's information. Various privacy policies and tracking cookies will be referenced as widely used tools of attack. Finally, suggestions for further research and action will be suggested.

Organization of the Project. This project is organized as follows: Chapter 2 will provide the literature on common techniques and practices used by companies to infringe on your privacy. Chapter 3 will provide suggestions on the how to answer the three questions that the project proposed. Chapter 4 will provide the data samples from the suggestions that were provided in Chapter 3. Finally, Chapter 5 will provide a discussion of the results and suggest areas for further investigation.

CHAPTER TWO:

INFORMATION PRIVACY

Information Privacy Defined

The big five technology companies are tracking, collecting, and selling their user's information every day to fuel the $227 billion-a-year industry. The worst part of it all is that the average user is unaware of these acts that are infringing on their privacy. There are many ways that these technology companies are able to infringe on the information privacy of a potential user. Offering "free" software and device fingerprinting are two primary ways that technology companies are able violate the user's information privacy.

All of the big five technology companies have one goal. That one goal is to collect as much information about their users as much as they can. One of the ways the technology companies achieve this goal is to provide users a free service. In order for a user to use that free service they must agree to the companies' Terms of Service and Privacy Policy. However, the Digital Journal in early 2020 reported on a survey that ProPrivacy published that showed " that only one percent of users read the terms and conditions before clicking the accept button "(Digital Journal). Those who read the Terms & conditions will understand how their information is being collected and sold in order to keep these products and services free for them to use. Let's have a look at Amazon which is one of the biggest retail company in the world.

The Fortune 500 “ranks Amazon as the second biggest company in the world just behind Walmart”(Fortune 500). There are three major ways that Amazon violates their customer’s data. Amazon has a database on their customers from information collected form Amazon Web Services (AWS), IoT devices, and their own ecommerce website. AWS is so big that it is reported by Forbes that “nearly one third of the internet’s traffic running through AWS”(Runkevicius1). Amazon even has their own personal AI named Alexa. Alexa is built into majority of their IoT devices which gives the customer with ease of use. The website Choose to Encrypt states goes into detail on how “Alexa is one of the biggest privacy issues that faces Amazon”(Choose To Encrypt). TJ McCue of Forbes has reported that “Alexa has been caught on snooping on user's conversations that have nothing to do with Alexa”(TJ MacCue). The article continues stating that “with those recorded conversations Amazon is able to market and advertise certain products to their users that has been mentioned in the recorded conversations that Alexa has recorded”(TJ MacCue). Alexa has also been recording and storing user's conversation that was between the user and Alexa. Those conversations are later being analyzed by Amazon employees. There are even privacy and ethical concerns with the Amazon Fire Operating System which is the Operating System that runs on all of the Amazon Fire Tablets. The Amazon Fire Tablets have a camera, microphone, and location tracking software. All three of these features are there so that Amazon is able to access and collect information about your device usage. The

unfortunate thing about this is that the Amazon Fire Tablets is that it is marketed to children. This is bad thing because this allows Amazon to advertise products and services to them. Now it is time to go over Google's Privacy problems.

Any of Google's free products would fall under the Google Terms of Service. Within the Google's Terms of Service, it is clearly stated that you are giving Google permission to “host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute anything that you do under the Google suite of products” (Google). This does include (but not limited to) Hangouts, Photos, Docs, Drive, and Gmail. Google also tracks potential users even if they do not visit or use any off the Google services by allowing websites to run Google analytics code. This code allows Google to track visitors from specific websites and are able to create a historical map of most of the internet activity of its users. Google is even in completion within the AI space with their own AI that comes standard with their own IoT devices. Now, I would like to go into detail about Facebook and their Privacy Policy.

Facebook is the largest social media company in world. Since 2004 there have been three major acquisitions that Facebook has partaken in. Those acquisitions involved Instagram, Oculus, and WhatsApp. What Instagram, Oculus, and WhatsApp have in common is that they all fall under the same Facebook's Privacy Policies. Within the privacy policy of Facebook, it is clearly states how they collect user date: "We collect information about how you use our

Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities" (Facebook). This means that legally, Facebook is allowed to record and monitor any user's activity that uses their products and services. This does include the activity that is generated within the popular secure messaging app WhatsApp. Facebook also tracks its users when they leave their site with Tracking cookies. Tracking cookies are also another way for the technology companies to invade their user's information privacy. These tracking cookies collect a trail that a user's device leaves onto a website. Now I would like to go over Apple, and Microsoft whose main source of revenue is hardware.

Apple is one of those Technology companies that strongly supports privacy. Their privacy policy sites states that "privacy is a fundamental human right" (Apple). However, it seems that is too good to be true. Since 2020, Apple dropped its plans to allow their iPhone users to fully encrypt their backups on their own devices before uploading those backups on the iCloud. This includes (but not limited to) text messages, calendars, photos, and contacts. Two years ago, Forbes reported that "Apple was caught hiring employees to listen into Siri conversations without the user's consent" (Su 1). Apple quickly issued an apology to its users and promised that it would never happen again. However, a whistleblower from the Guardian revealed that nothing has changed and that Apple employees are continuing to ignore their own policies. It seems to me that

Apple is being loose with their Privacy Statement with each passing year. Now I would like to dive deep into how Microsoft keeps a tab on their user's privacy through their products.

Microsoft makes its money by selling gaming consoles and licensing their Operating System to 3rd party companies to use on their hardware. Windows 10 is the most recent Operating System that Microsoft has released in July 2015. Within the past seven years it has been reported by Fox 8 news that “Windows 10 is considered to be a privacy nightmare for all of its users” (Fox 8). The first major privacy issue that Windows 10 assigns each device with an automatic advertising ID. That ID can be used by the hardware and software companies to generate tailored ads for the user to see. These ads will also be tied into Microsoft Edge for those companies to advertise their products to potential users to lure them into their website. Requiring a Microsoft Account to sign in is also a major sign of a privacy breach. Having a Microsoft account tied to your device would allow Microsoft to collect, analyze, and store information about how their users use their device and operating system along with their AI personal Assistant Cortana. Lifehacker reported that “Cortana is also another privacy concern due to the fact that it collects and stores information on how the user interacts with Cortana”(Gordon

CHAPTER THREE:

SUGGESTIONS ON HOW TO PROTECT ONES PRIVACY

This project will go over three technology solutions that can mitigate privacy infringement by the big five technology companies. Majority of these solutions would be coming from Michael Bazzell's book "*Open Source Intelligence Techniques 8th Edition*" alongside "*Extreme Privacy What it takes to Disappear 2nd Edition*". Each of these solutions that are outlined can range from low to high-cost solutions. First, I would like to provide a table that will cover some of the essential software that will be considered in each cost solution. Then I will go over each product individually to provide an understanding of how they would combat the threat of information privacy that the big five technology companies.

Table 1. Software Usage during this Project

Product Name	Product Purpose	Product Price
ProtonMail	Email	$6.25/month
Standard Notes	Note Taking	Free
Signal	Messaging Application	Free
VeraCrypt	Encryption Software	Free
Mozilla Firefox	Web browser	Free

Software Options

Proton Technologies is a company based in Switzerland that provides an open-source email service called ProtonMail. “ProtonMail is known to be a zero-knowledge email provider with end-to-end encryption” (ProtonMail). This means that email that is stored and sent out via ProtonMail are stored in a way that Proton Technologies are not able to view or read anyone’s email. By having this "zero-knowledge" feature Proton Technologies will not advertise, sell, or collect any of their user's information to third party companies. ProtonMail has two tiers for a person to choose from. There is a free tier which limits a person to only 500 MB in email storage or a paid plan for a monthly fee of $6.25. This project will be using both plans and which would be included in the overall Technology Solutions. Now it is time to explain why this project has chosen ProtonMail as their main encrypted email storage over their competitor.

By examining this given table, we are able to see some clear differences between the major email providers

Table 2. Comparison Table of Email Providers

Name	Parent Company	Company jurisdiction	Privacy Policy site
Gmail	Google	USA	https://policies.google.com/privacy

Outlook	Microsoft	USA	https://privacy.microsoft.com/en-us/privacystatement
ProtonMail	Proton Technologies	Switerland	https://protonmail.com/privacy-policy
Apple Mail	Apple	USA	https://www.apple.com/legal/privacy

One of the most interesting differences is that ProtonMail is the only email provider that is outside the United States. The thing about Switzerland is that it is not apart the Fourteen Eyes Agreement. The Fourteen Eyes Agreement is an electronic surveillance program on a global scale. These fourteen countries "focus on intelligence gathering, counterintelligence operations, and law enforcement by intercepting communications and other electric signals". This means that there is a good chance that your digital activity is being shared with the NSA or other security agencies if you do any suspicious electronic communication within the fourteen countries. A privacy haven has been created in Switzerland since their country has opted out in the agreement. The Proton Technologies' suite of products are the only Products that are on this list that are located outside of the United States of America. Next, we will be focusing on the note taking application that will be used.

Standard Note is an open-source application that is end-to-end encrypted notepad that is available on all mobile devices. Standard notes are also zero-knowledge and that the company who is behind standard notes will not be able

read the notes that their users have created on their device. On January 5, 2021 Mo Bitar published the latest Pent Test and security audit. Mo stated that “that they are pleased with the results, and their impact on making Standard Notes the most secure Note-taking application available” (Mo Bitar). The messaging app is the next piece of software that I would like to go over.

By taking a look at this table that is provided by securemessaging apps we clearly see some major differences between them.

Table 3. Comparison Table of Messaging Applications

Messaging Application	Company Collects User Data	Company jurisdiction	Funding	App collects customers' data?	Are the app and server completely open source?
Google Messaging	Yes	USA	Google	Yes (Difficult to assess given the app is integrated into Google's greater ecosystem)	No
Apple IMessage	Yes	USA	Appe	Yes (Difficult to assess given the app is integrated into Google's greater ecosystem)	No
Facebook Messanger	Yes	USA	Facebook	Health & fitness / purchases / financial info / location / contact info / contacts / user content / search history / browsing history / identifiers / usage data / sensitive info / diagnostics / other data	No
WhatsApp	Yes	USA	Facebook	Health & fitness / purchases / financial info / location / contact info / contacts / user content / search history / browsing history / identifiers / usage data /	No

				sensitive info / diagnostics / other data	
Signal	No	USA	Freedom of the Press Foundation / the Knight Foundation / the Shuttleworth Foundation / the Open Technology Fund / Signal Foundation (Brian Acton)	Contact Info	Yes

One thing that is clearly visible is that majority of these messaging apps collects its user data. According to the Signal's website it states that "Signal with its "State-of-the-art end-to-end encryption" which is powered by an open-source signal protocol keeps all of the conversations secure" (Signal). The website goes into detail about how "every call and text message will not be intercepted and transcribed by signal. There is no ads on this messaging platform or even trackers that will track your location when using Signal to message with". The best part is that signal is free and available on every mobile device. This is because Signal is nonprofit which is not tied to any major technology companies. Signal is supported grants and donations from its users. It is very important to keep all of our information safe and secure when it comes to all the files that we create on our laptop.

VeraCrypt is an open-source program that allows the users to encrypt all of their devices and files. VeraCrypt allows the user to download and maintain their encryption keys on removable storage. This storage process is done because it allows the user to move their files freely from one device to another. Web browsers are going to be the last piece of software that will be covered. By Taking a look at this table that was provided by Mozilla we are able to compare the top web browsers.

Table 4. Comparison Table of Web Browsers

Product	Private Browsing mode	Blocks third-party tracking cookies by default	Funding	Web extensions/Add-ons
FireFox	Yes	Yes	Mozilla foundation	Yes
Edge	Yes	Yes	Micrsoft	Yes
Chrome	Yes	No	Google	Yes
Brave	Yes	Yes	Brave Software	Yes
Safari	Yes	Yes	Apple	Yes

Mozilla Firefox will be the browser of choice. The reason for this is because Mozilla Firefox is an open-source web browser that allows users to browse the web with privacy in mind. Mozilla Firefox is considered to be most personalized web browser that is available. Ad-ons and browser tweaks are just a few ways that you can customize Firefox to your liking. Here is a list of Ad-ons and tweaks that were provided by Privacytools.io which is a website that helps users

maintain their digital privacy. I would recommend for any user to use to maintain their Information Privacy when using the internet.

Table 5. Firefox Add-on List

Add ons	Purpose
HTTPS Everywhere	Force HTTPS encryption on non HTTPS websites
Decentraleyes: Block Content Delivery Networks	Decentralizes emulates Content Delivery Networks locally by intercepting requests, finding the required resource, and injecting it into the environment. This all happens instantaneously, automatically, and no prior configuration is required.
ClearURLs	ClearURLs removes tracking cookies from URLs to help protect your privacy when using the Internet.
Terms of Service; Didn't Read	Grade's websites based on their terms of service agreements and privacy policies. It also gives a short summary of those agreements.
Snowflake	Snowflake is a new pluggable transport from the Tor Project. If you have an uncensored connection, running this extension volunteers your connection to be used as a Snowflake proxy to help users unable to connect to the Tor network. Your IP will not be visible to the site's users visit using your proxy, as this extension will not make you an exit node. If your access to the Tor network is blocked, this extension will not assist you, and you should use the Tor Browser instead.
Firefox Multi-Account Containers	Firefox Multi-Account Containers allow you to create containers for specific websites. These containers are isolated from each other.
Bitwarden	Password Manager

Source: Privacytools.io

Table 6. Firefox Tweak List

Tweak	Purpose of Tweak
privacy.firstparty.isolate = true	A result of the Tor Uplift effort, this preference isolates all browser identifier sources (e.g. cookies) to the first party domain, with the goal of preventing tracking across different domains.
privacy.resistFingerprinting = true	A result of the Tor Uplift effort, this preference makes Firefox more resistant to browser fingerprinting.
privacy.trackingprotection.fingerprinting.enabled = true	This is Mozilla's new built-in tracking protection. One of it's benefits is blocking tracking (i.e. Google Analytics) on privileged pages where add-ons that usually do that are disabled.
browser.send_pings = false	The attribute would be useful for letting websites track visitors' clicks.
dom.event.clipboardevents.enabled = false	Disable that websites can get notifications if you copy, paste, or cut something from a web page, and it lets them know which part of the page had been selected.
media.eme.enabled = false	Disables playback of DRM-controlled HTML5 content, which, if enabled, automatically downloads the Widevine Content Decryption Module provided by Google Inc
media.gmp-widevinecdm.enabled = false	Disables the Widevine Content Decryption Module provided by Google Inc., used for the playback of DRM-controlled HTML5 content.
network.IDN_show_punycode = true	Not rendering IDNs as their Punycode equivalent leaves you open to phishing attacks that can be very difficult to notice

Source: Privacytools.io

Hardware Options

It is time to go over the hardware that I would recommend to a user. This list too can be found within the “Open Source Intelligence Techniques 8th Edition”. this list I will be listing a group of electronics that will be in a form of computer. Each of these hardware devices will have tweaks on them in order to maintain their privacy against the five major technology companies.

Table 7. Hardware Usage during this Project

Product Name	Product Purpose
Macbook Pro	Computer
Windows	Computer
Raspberry Pi	Server
Synology DS920 NAS	Server
Western Digital 2TB External Hard Drive	External Hard Drive

There are many options to choose from when it comes to what type of laptop that you would like to use. Apple, Linux, and Microsoft are the three different operating systems to choose from when deciding what laptop to choose from. If you decide to go with a Windows laptop here are some of the recommendations that I would make. The best recommendation for a new

Windows device would be to follow page fifty-six in the “Extreme Privacy What it takes to Disappear 2nd Edition”.

Page fifty-six in the “Extreme Privacy What it takes to Disappear 2nd Edition” it states that “ Typically, Windows 10 will come preinstalled when you buy a new Windows laptop”(Extreme Privacy). Then the book goes into detail about how to reinstall the Operating System with Windows 10 LTSC. Windows 10 LTSC is a Windows 10 Operating System that does not include Cortona or any of the Windows’s bloatware that any Windows 10 Operating System comes with. It is extremely important when making an account for your laptop make sure you make an offline account. This offline account will not require you to make or sign into a Windows Account. Once the off line account has created then I would download Signal, Standard Notes, Mozilla Firefox, and VeraCrypt. I would then use VeraCrypt to encrypt the entire disks space along with creating a 1 TB container to store all of my important files in. One of those files would be the encryption keys for the Encrypted System volume that we have just made. Now let’s take a look at how setting up an Apple computer.

Make sure that you do not sign into an Apple account when making an account for your device. When you make a local account on your computer then you are limiting information that is being collected by Apple. There are some drawbacks when you create an offline account for your Apple device. One of those drawbacks is that you will not be connected the Apple ecosystem. Because

of this you will not be able to receive iMessage or phone calls that are coming from your iPhone. By Using the Signal application on your mac will fix this problem. Another drawback is that you are not able to download any applications from the app store when operating on an offline account. You would need to download the application from the developer's website. For the Mac I would download Signal, Standard Notes, Mozilla Firefox, VeraCrypt, Little Snitch, and Outline. Little snitch is an application firewall that will tell the user what application is running and what information the application is sending off to their company. There the user can instruct the application not to send out data to their company of origin. The Application called Outline is a private alternative to OneNote. It is time to take a look at one of the most popular single board computers on the market.

The Raspberry Pi is one of the most popular single board computers on the market. There is currently a 4th Edition of the Raspberry Pi. For this project I will be using the Raspberry Pi 4 with 8GB of RAM and it currently stores 128 GB of storage. I will also have a Western Digital Portable Hard Drive attached to this unit for it's storage capabilities. The Raspberry Pi will be acting as a personal cloud service. NextCloud would be the cloud software that would be running on the Raspberry Pi. NextCloud is an open-source cloud program that turns any computer into a personal cloud service. With NextCloud it is possible to take control back of your data and not allow it to be seen by third parties or a major

company. Now it is time to take a look into a more expensive Personal cloud option.

The Synology DS920 is a home server that is made by Synology. This home server is packed with a full suite of products in which can help anyone start and manage their very own home server. The Synology suite of products includes Synology Drive, Synology Photos, Synology Calendars, and Synology Audio. The Synology Drive allows anyone to upload files from any device to make sure that they are backed up. Sinology Photos allows users to back up their own photos and videos to the could itself. Synology Calendars allows each user to set their own calendar and share it with other devices. Finally, the Synology Audio is a place where users can upload their music to and create their very own radio station to listen to offline.

Pricing Models

Since going over the main hardware and software that would be used in each technology solution. Here are the three cost solutions that this project has covered over the span of six months.

Table 8. Low End Cost Solution

Product Name	Purpose	Cost
Signal	Text Message	Free
Standard Notes	Note Taking	Free
VeraCrypt	Encryption Software	Free
ProtonMail	Email	Free
2 TB Western Digital	External Storage	$60
Mozilla Firefox	Web Browser	Free

Table 9. Medium Cost Solution

Product Name	Purpose	Cost
Signal	Text Message	Free
Standard Notes	Note Taking	Free
VeraCrypt	Encryption Software	Free
ProtonMail	Email	$65
2 TB Western Digital	External Storage	$60
Raspberry Pi 4	Personal Cloud Storage	$61
NextCloud	Cloud Storage Software	Free
Mozilla Firefox	Web Browser	Free

Table 10. High End Cost Solution

Product Name	Purpose	Cost
Signal	Text Message	Free
Standard Notes	Note Taking	Free
VeraCrypt	Encryption Software	Free
ProtonMail	Email	$65
2 TB Western Digital	External Storage	$60
Synolgoy DS 920 with 14TB	Personal Cloud Storage	$1300
Synology Software Suite	Cloud Storage Software	Free
Mozilla Firefox	Web Browser	Free

CHAPTER FOUR:

ANALYISING THE DATA SAMPLING

All three of the pricing models have been tested and tried numerous times throughout the past six months in hope that I can disappear myself . The results of each these models are very different and each of these pricing models have their own drawback and advantages of each which does not include the price factor of remaining model.

Storage

When it came to storing my data, I wanted to make sure that I am able to have quick access to it and it would be able to sync to my various devices. When it came to storage options, I wanted to make sure that full disks encryption is relativity available and easy to set up. That is why all three price models that I have recommend the user to store their information in different ways. The first way was to store their information into an encrypted container on a personal external hard drive. The next two storage options were to use two separate on-premises cloud storage solutions. One of those ways was to use an open-source service and the other a cloud source system. The first thing that needs analysis is the personal hard drive.

Portable Hard Drives. Ease of use and secure were the two major reasons why using a portable hard drive for backup was the easiest thing to do. However, it was time consuming when setting up this device. The setup process

with using VeraCrypt on the portable hard drive took the longest. The reason for this is because VeraCrypt needed the time and resources of the host machine in order to make the encrypted container. It took just about five hours to create a standard encrypted container onto my portable hard drive. Once you have your portable hard drive setup with VeraCrypt then you are all ready to backup any device that is connected to it. Having to constantly be connected to the hard drive for a backup to complete can be annoying and frustrating when wanting to obtain access to an important document or file when one is out and about. That is why between the excessive downtime and lack of accessibility are the two major reasons why I would not recommend this method to anyone who is constantly on the go and who needs access to their data quickly and effectively.

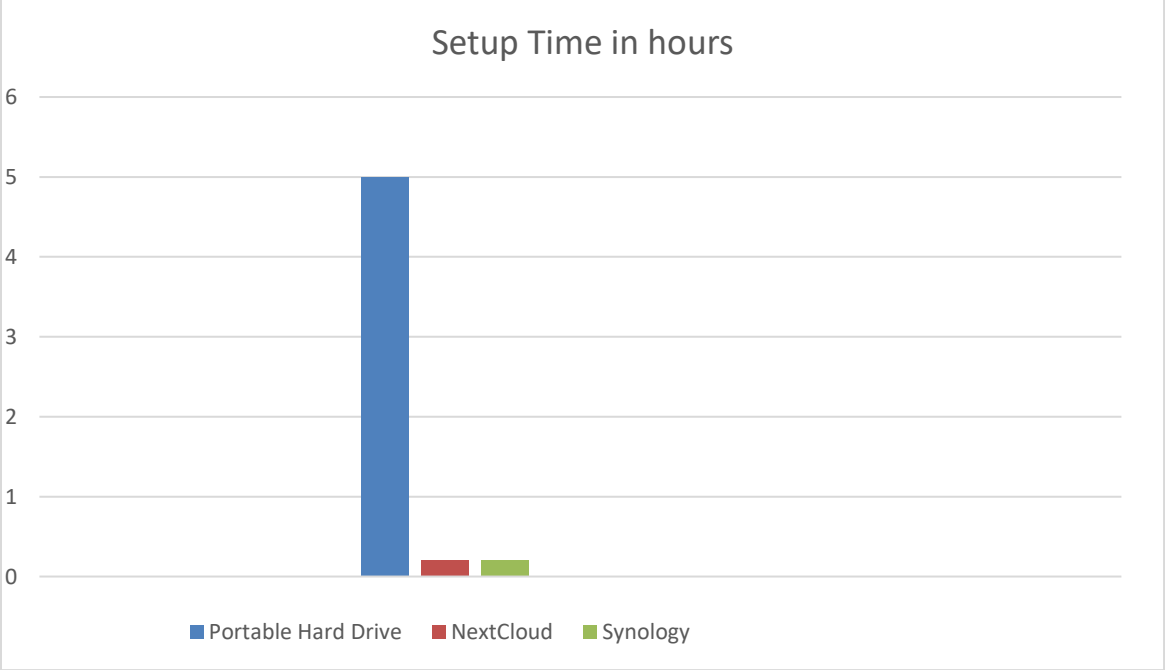

Figure 1. Setup Time Comparison.

Now both of the long setup times and accessibility issue can be solved by using a cloud service.

Table 11. On-Premise Cloud Comparison

Provider	Price	FDE Available	Open-Source?	Mobile Apps	Multi Authentication	Auditing	Customization
Next Cloud	Free	Yes	Yes	Yes	Yes	Yes	No
Synology	Induced with purchase of Synology device	no	No	Yes	Yes	YEs	No

When it comes to cloud storage it is important to keep the privacy mindset. With the privacy mindset it is important that we keep our data on an on-premise cloud. The table provided below lists the two on-premise proiders that I used. . NextCloud is the first on-premes provider that I would like to go over.

NextCloud. The first on-premises cloud that was used in this project was called NextCloud. NextCloud is an open-source cloud storage platform that can be configured on any device. For this project I was able to configure a Raspberry Pi 4 to be able to run and maintain NextCloud. In order to do this, I had my Raspberry Pi 4 run an Operating System called NextCloudPi. The install process

took 12 minutes. NextCloud was ready once I inserted the Operating System into the Raspberry Pi 4.

What I loved about the NextCloud was that it was secure, accessible, and adaptable. This On-premises cloud allowed the device to be fully encrypted and had many options that the user can configure to make sure that they had the perfect setup in place for their storage. The best part of it all was that you can have access to this device anywhere you want. However, this service did require a lot of time to keep this device up to maintenance and standards. Since this service was open source and was built by a community of people. If an issue ever occurs in any form, it would take weeks or months for someone to develop a solution to that one particular problem. Now if this cloud service would be fully funded cloud source, then the downtime for a problem that need fixing may not be a problem at all.

Synology NAS. The higher end pricing model tested a Synology NAS when it came to storing important documents. The nicest part about the Synology NAS is that it is reliable, accessible, and adaptable. However, for being a closed system there was a lot of features missing that should be needed in order to truly become the replacement for any online cloud storage. The different rules of the different roles were not fully configured on this device. Lack of customization was also a big downside of this device. The lack of Full Disk Encryption (FDE) on this NAS was the biggest disappointment to me. Overall, I truly think that Synology has a lot of work to do and a lot of features to enable in order to be the best

replacement for any online cloud storage. Now it is time to go over the types of laptops that were being used to access these storage service

CHAPTER FIVE:

DISCUSSION AND FURTHER RESEARCH

The five major technology companies all profit on violating their user's privacy and selling their information to third parties. With a world full of data, where almost everything is being stored and analyzed in a database is everywhere, more techniques and tools are needed to protect the user's privacy in hopes of minimizing the data collection on unsuspecting users. Current methods of using everyday hardware and software that are funded by the big technology companies are no longer producing the results. Applying additional hardware and software that are not funded by the major technology is one way to solve this problem and add another line of defense in maintaining privacy.

This project posed the following questions:

1. What are some common techniques that Amazon, Apple, Microsoft, Facebook, or Google use to gain personal information?
2. At what cost would it take for someone to maintain their privacy online without interacting with Amazon, Apple, Microsoft, Facebook, or Google?
3. What are some reasonable recommendations would I recommend to the average unsuspecting user?

Result 1: Privacy Policy, tracking cookies, and freeware are Some Common Techniques to Gain Personal Information. Unsuspecting users need to pay attention when they are signing up for a any product or service. The unsuspecting user should be concerned on what information is being collected. Informing users of these potential risk can help remediate the collection process of data. Finally, users should consider of using alternative hardware and software in order to achieve the same desired goal.

Result 2: An Average User Can Pay Enormous Amount of Money to Maintain Their Privacy. The cost of maintaining privacy can fluctuate depending on the importance for the user to maintain their privacy. Within Chapter 3 outlines some key pricing models. As these companies evolve over time the cost of maintaining privacy will as well.

Result 3: Using a combination of open-source and periptery software is my recommendation for the average unsuspecting user to use,

With the evolving world of information technology and the technology companies behind them, there are many more steps that a user can tale to strengthen their privacy. With the unknown of the future of these IT technology companies must be considered, and research pursued. Suggestions for future research in geofencing capabilities can be found in Appendix A.

APPENDIX A:

SUGGESTED FUTURE RESEARCH TOPICS

Adding cell phones to this research would be an excellent idea since it is the device that people used most often. Adding the phone model and operating system would make a major impact on if the user will be pinging the major technology companies since majority of the phones rely on Google, Apple, and Microsoft as an operating system. Replacing a phone number with a Voice Over IP (VOIP) number would also be an interesting research area since the cell phone companies keep a record on its customers while storing all of the information that is being sent and received over the phone. If a user does not think about redundancy when using their phone then there will be a problem to restore backups.

The number one rule in IT is to always make backups of your devices. Now taking that rule a step forward we would need to think about making backups for our backups in case something fails overtime. Compiling a list of redundancy options for this privacy project would be an excellent idea because we would want to make sure that our products and services are always accessible when we need it. Now, it would be interesting if a faraday bag was thrown into the location as a form of pure privacy.

REFERENCES

Open Collective Foundation. *PrivacyTools - Encryption and tools to protect against global mass surveillance - https://www.privacytools.io*. 2020. 1 April 2021.

Apple. *https://www.apple.com/privacy/*. n.d. 20 April 2021.

Bazzell, Michael. *Extreme Privacy: What It Takes to Disappear*. 2020.

—. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. 2021.

Bitar, Mo. *Standard Notes Completes Penetration Test and Cryptography Audit*. 5 Junaary 2021. 20 April 2021.

choosetoencrypt. *Privacy Issues with Amazon*. 11 September 2019. 20 April 2021.

Facebook. *Data Policy | Instagram Help Centre"*. n.d.

Fortune500. *https://fortune.com/fortune500/*. 2020.

Google. *https://policies.google.com/terms?hl=en.* n.d.

Gröne, Florian, Pierre Péladeau,. *Tomorrow's data heroes,*. 2019.

https://protonmail.com/security-details. *security-details*. n.d.

IAAP. *https://iapp.org/about/what-is-privacy/*. 2021. 20 April 2021.

McCue, TJ. *Amazon Alexa Accused Again Of Spying: Here Is Another Solution*. 30 July 2019. 20 April 2021.

Runkevicius, Dan. *How Amazon Quietly Powers The Internet*. 3 September 2020. 20 April 2021.

Sandle, Tim. *http://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127.* 29 January 2020. 20 April 2021.

Signal. *https://signal.org/en/*. n.d.

Su, Jeb. *https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-apple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recordings/?sh=6afe5b1e7314*. 30 July 2019. 20 April 2021.

WIRE, CNN. *https://myfox8.com/news/is-windows-10-really-a-privacy-nightmare/*. 17 Aug 2015. 20 April 2021.