HOW CAN WE STOP COMPANIES FROM GATHERING OUR DIGITAL DATA AND SELLING IT AND MAKING A FORTUNE?

Prepared for

Dr. Christine Choi

Prepared by

Edward Acevedo
Jerson Vargas
Turjo Chowdhury
Djeneba Bah

TABLE OF CONTENTS

HOW CAN WE STOP COMPANIES FROM GATHERING OUT DIGITAL DATA AND SELLING IT AND MAKING A FORTUNE?

SECTION 1

INTRODUCTION

Turjo Chowdhury

Technological progress is seen as nothing but a blessing to mankind. The advancement of technology has made concepts that were science fiction 50 years ago into reality today. From Rovers exploring extraterrestrial planets to the microprocessors that control smart phones in our hand, everything has been possible for the expansion and development of technology. For everything to be where they are today, the internet has undeniably been the main instrument that made everything possible. Communication and transmission of data was what the internet was primarily developed for and today it is what keeps every human running. From news to social media, research to entertainment, we blindly rely on the internet today and that dependence is what some companies secretly use to gather data. Such data can contain information such as interest, personal preference, location data, demographics etc, and are collected without the knowledge of the users. The collection of data is then sold to other companies and can be used, for example, for marketing purposes to curate targeted advertisements. The use of the internet has made us victims of stealthy data collection which eventually gathers information which can be used for targeted purposes. As we discuss our topic through this paper, we will be discussing the some main points that we see with this worldwide issue. The overall discussion of this project is even though we can't permanently stop companies from gathering our personal data. We want to show what are some preventative measures that can be taken to lessen the collection of data.

OBJECTIVE OF THE RESEARCH

Jerson Vargas / Edward Acevedo

The objective of the research is to design a report explaining multiple solutions on how and why companies are collecting our personal information and data and selling it to fortune one

companies. Additionally this research is also designed to show everyday users that we are not safe, people and companies are always watching us and we as users don't even see it happening. We the people are far from having our own privacy when it comes to these electronic devices, we are always being watched. For example there are companies that collect our facial expressions and our voice and our environment that we are in. These companies are not only out to get our personal data there are companies that want to collect our personal appearance, even our DNA. A company such as Google, uses their social media platforms for example they use YouTube to collect our cookies and cache. To see what video we as users are watching and see how we interact with the environment, they are basically looking for our needs and wants. By companies taking this information they go through it and basically start pushing advertisements onto the user that are related to things they have seen and searched for in the past. Also there are companies out there that make most of their revenue by putting out Ads onto their platform. Companies have a data log of everything users do on the platform, if we get into detail companies can collect our payment information, search history, pictures we've liked and commented on, they can even monitor the device ip you are on. This is a total breach of our privacy. Thus this paper will illustrate a detailed description of things you will see with companies and what they do with all the data they collect from their users. It will also show what are some steps that we as users can take to minimize our exposure to these companies.

METHODOLOGY

Edward Acevedo

As we were doing our research there were many things that we had to factor in to narrow our research. We as a team had to brainstorm key terms to really narrow what specifically we want to talk about throughout our paper. Some of those terms we came up with that will help us narrow the search are digital data, cookies and cache, youtube algorithm, data breaches, data collectors, digital ads, and google collecting personal data. We were able to come up with this list that describes the overall idea of our topic, once we came up with our list we began doing our research. We began by utilizing the New York City College of Technology Library Database, we started by doing deep searches using our list of key terms we came up with as a team.

As we began doing our search we looked for certain articles that pertain to the topic we narrowed the search we used the filter tool that the search engine offers. For example the filters that one of us used as we did our search was, we searched digital data as the main search criteria we then

added selling, also privacy. We narrowed the search by selecting only articles that were published from 2017 to 2022 and that are related to science & technology and technology. We as a team were all able to come up with at least one to two articles using our own filters that really describe the overall picture of the issue we are trying to let the world know. Each of us spent a good amount of time skimming through articles that best fit our topic. Throughout this paper, we will be utilizing these articles to describe this worldwide issue that we believe is impacting us everyday users. A method we talked amongst each other, it pertains to our research. We knew that the research we all were going to find was going to be repetitive, that we were mostly going to find similar or the same information pertaining to this topic. So what we discussed amongst each other was lets each talk about different companies, whether it be Google, Facebook, Tik Tok, Instagram, etc. So what this means is as we do our research we are trying to look for information that pertains to these companies. The reason being is because each of these major companies utilize or use their users' data in different ways.

RESULTS

Edward Acevedo

After doing research this topic has given me a better understanding of our data privacy, it has shown me that we as users of the internet are vulnerable. From entertainment applications to social media applications, or any kind of applications that we use on our devices, any information we put out there, it's out there for people to get knowledge of. It's ridiculous to think that any kind of applications we use all collect some kind of data whether it be personal information, facial expressions, our activities, location information, etc the list can go on and on. As I was doing my research and adding my filters I came across articles that stood out to me the most, the first article was from Michael Sengelmann known as “An overview of Reverse Engineering and A Security Analysis of Tik Tok”. This author explains the importance of data collection and what it does for companies. The author also explains how data collection is done through users consciously knowing it's happening. This author also explains how technology is advancing our footprint we leave on the internet is more than basic information. This article gives great examples and discusses important key points that I want to include in the overall discussion. The second article that I came across was by Stachl C., Boyd R., Horstmann K., Khambatta P., Matz S., Harari G. known as “Computational Personality Assessment”. As I was

researching this article, it gave great examples using the former director of monetization of Facebook, which gives us as users a better understanding of what these social companies are thinking. This article discusses a bit about Facebook tactics such as what they do to lure their users to stay on their social media platform. Overall my findings regarding this topic were mind blowing there is a lot to talk about and discuss which I will talk more about in the discussion section.

Djeneba Bah

This whole research was much like awakening to me. Throughout my research, I first learned that humans are the most vulnerable asset in the technology era. I looked at the vulnerabilities in various aspects. Then I ended up learning about the main reason for this paper, which is how to reduce the vulnerabilities. The following are some of the many ways to protect our personal data: One can accept all the cookies to protect themself from online threats, the good thing is that most websites have it now. Secondly, changing your browser privacy more often is crucial, making sure you're not Opt-in of targeted ads, with that being said computer users might consider using an ad blocker. Last but not least, opt out of data broker sites that sell your personal information.

Jerson Vargas

After researching the given topic at hand, our data is one of the main sources used for big companies to steal and to target certain ads on us based on what we search up. It is best to try and keep your data stolen as little as possible. Things on websites such as cookies and what you click on websites are just examples of the harm that can be done. Companies such as Google, Microsoft, etc, can even go on, reaching as far as stealing a person's health data. One way this occurs is due to algorithms companies use to target a certain user based on what they search. Based on Wilbanks," Stop the Prevention of Health Data". Google uses an algorithm known as "Knowledge Graph, so that users obtain information that is more relevant and supposedly more accurate whenever they type in their symptoms or condition. The service (which for many ailments may replace visits to the doctor) will only enhance Google's — and only Google's — ability to conduct an unprecedented level of information retrieval for health." This is just one example of how powerful tech is in the real world. Even today, to access many buildings, facilities have used technology to allow contactless entry into the real world. This happened due to the events of the pandemic. Based on Whitelaw, et al. in "Applications of digital technology in COVID-19 pandemic planning and response"Several digital health interventions, particularly

those that track individuals and enforce quarantine, can infringe on privacy, while increasing risk among individuals with mental illness or restricted access to food or water. Government-implemented surveillance and control can instill fear and threaten civil liberties."

Turjo Chowdhury

After doing my research on the topic, I was able to understand how data is collected and how we are forced to comply. From the periodical "Are You Being Watched?" from the magazine Scholastic Scope published in 2017, The more information a company has on us, the more successfully it can sell to us. What I found surprising was in the magazine periodical, it is mentioned 75% of the websites save our data. The data that is being stored ranges from interests to our location history which I think is very alarming for most of the population and what makes it more disappointing is the websites and apps are curated in such a way that they need all this user info inorder to work the way they are supposed to. The best way for us to protect our data is basically refraining from using the services but then we lose the luxury of information that we can have in the palm of our hands. The article "The price of free: how Apple, Facebook, Microsoft and Google Sell you to advertisers" by Mark Hachman highlights what free means in today's world wide web. The author points out how the technology giants of the world today collect and sell our information in disguise of free service. What I find astonishing is that most of the users live under the illusion of free services where they are far away from freedom. Facebook being one of the main collectors of data, collects not only what users are interested in, but also what their friends say about each other. This makes us question, what doesn't facebook know about us? Facebook makes it easy for us to connect with friends and family. We can make calls, send pictures and texts, post pictures and react to each other's posts but at the cost of giving up our personal information. Google, Apple and Microsoft also use certain terms and conditions which basically forces us to give information in order to use their products and services.

DISCUSSION

Turjo Chowdhury

The more information a company has on us, the more successfully it can sell to us. Development of targeted advertising is a large market with so much room for rapid growth. Businesses purchase monitoring data in order to develop targeted advertising and those advertisements are sent to people who are most likely to want the offered products or services. In the magazine

periodical “Are You Being Watched?” on scope.scholastic.com the author uses an example with which every user can relate. The author tells us about how we can be looking for a solution to a problem on google and the next thing we start seeing products and services related to the problem in all our social media. This is primarily done when we enable websites to send and receive cookies. The more information businesses have about us, the more successfully they can market things to us. There are a few options for limiting tracking and information collection. If users don't enable cookies, users will have to enter login and password each time you visit a website, which makes the experience of using the internet not as great and seamless. Also this would not disable every form of data collection. Using Google for example, we are forced to agree to their terms and conditions to use their services which includes agreeing to information being collected. In today’s world, the way Google is intertwined with the internet, Google is used more as a verb than a noun. We cannot imagine the internet without the existence of google. Sure there are other search engines but nothing compares to google. Privacy advocates believe that we should have more control over how information about us is collected and used. Using different search engines is one of the few ways we can minimize data collection.

According to the article “The price of Free: how Apple, Facebook, Microsoft and Google sell you to advertisers.” by Mark Hachman, businesses today have the idea of having every right to demand your personal information before starting any business. Although all these giant tech companies try to reassure us that privacy is their main concern, their actions, products and services show us it’s completely not true.

Reading through the article, we know that Facebook basically has every information possible from us through their products by collecting and monitoring our actions. We, as facebook users can do very little about it as the author mentions that even if we delete our facebook account, our data will not necessarily be removed because according to facebook, the information is “theirs”. Mark Hachman also highlights how Google and Apple collect our data. Apple's privacy policy does a poor job of describing what data it collects. Apple promises that they protect user data but the promise cannot be valid as information such as location is taken so much that users get notification of traffic updates even before they are on the route for a destination. Location history is collected and predictions are done based on location history. In terms of controlling how much data is collected, one thing mentioned is Apple let’s users reset preferences which means users would have to reset their data from time to time. It is not a permanent solution and as we have

seen with pretty much every other company, if we want to use it, the only thing we can do is to comply.Despite its sanctimonious attitude regarding advertising, Apple does not make it easy to opt out.

Reading through the article, Microsoft says that it does not examine your email for personal information but the author warned us not to believe it. The author explains the whole process on why and how Microsoft reads through the emails to collect data. Looking through all the examples given, All the tech giants who rule the tech industry give us nothing but false hopes. For us as users, our hands are tied if we are to use their services. Some alternate services do exist but the problem is they are not even close to the products and services offered by these huge companies.

Djeneba Bah

Based on what I found, It looks like there isn't any real solution on how to stop data collection. However, instead of doing a general search I searched on how Microsoft handles the matter of collecting data. As a result of that I learned that for Windows 10 users, you can actually deactivate/disable some features from your computer to minimize the data collection. When setting up your new Windows 10 P.C, you should be really mindful of which features to activate or not in order to protect your personal information. At the end, I will provide the link to the article that gives a suggestion of which features to keep active or not. Finally, it gives you a step by step on how to disable each feature to secure your data.

Jerson Vargas

Based on what we have found within the results, our story tells us that there is no real way to solve or stop companies from stealing our data due to the fact that it is part of the monopoly of how companies make money and sell targeted ads to users, etc. Most big companies we have such as Google, Microsoft, IBM, etc. make money off of stealing our data for more than just entertainment purposes. It is really mind boggling how companies can steal information on our own physical health and on what location we are at a specific time. It is important to understand how impactful big data really is and how it affects everything we do in our lives. From work to health, to even daily interactions in our lives. Big Data controls ones.

Edward Acevedo

After a deep investigation I am amazed at what I have found. It's breathtaking to understand that anything we do on our smartphones, computers, and tablets all contributes to these companies

that collect our data. There are companies that inform the user of the kind of data they are collecting however that is not speaking for every company because there are companies that just take the data without informing the user. So just be aware that everytime you install an application, scroll through any of your social media platforms that some kind of information is being taken from you whether you know it or not. As I was doing my research I took a deeper dive into social media companies and how they utilize their users' data and information. The first article that stood out to me was from Michael Sengelmann known as “An overview of Reverse Engineering and A Security Analysis of Tik Tok”. Reading through this article, a sentence from the article “Social media platforms dominate the technological world." This sentence stood out to me because in many ways it's true. To basically summarize this article they talk about data security and state how important data collection is to social media companies. This article explains how companies steal our data consciously, what this means you users of social media platforms have most definitely seen this, whenever you install a new application and in order to use the application you have to accept the terms and agreement, and this can be for any kind of application not only social media application. Well inside the terms they mention the company is allowed to collect your data, whether you read it or not you have to accept the terms in order to use the application. So this is what it means when your data is being collected consciously, and whether you disagree to the terms what happens is it doesnt allow you to use the application. However this will never happen because there is a reason why the user installed the application to utilize it. As I went through these articles it showed that there is no permanent solution for this world wide situation. What I saw throughout these articles was ways to minimize our digital footprint. Some examples that were used in these articles are to use an incognito browser when you are on the internet. It will minimize the amount of data that gets collected. Another tip that I saw was to delete any unnecessary account that you might have, whether it be any random application that has asked you for personal information or even a social media application that you don't use. Another example that I think we all saw throughout these articles was the importance of VPN’s the reason why this is an important one is because whenever you are surfing through the internet any website you click into they can track your ip address of your device and sometimes are capable of getting your location. Overall we users of the internet need to understand that there currently is and won’t be a way to permanently remove ourselves from the internet, however there are many things that can be done to minimize our digital footprint.

CONCLUSION

Edward Acevedo

As we come to an ending to this discussion on this world wide situation we each have our own story to tell throughout this journey. We each were able to formulate our own story as we discovered more and more about this world wide crisis. We each were able to come together and discuss what our overall findings were. As I was doing my research I went down the road that dealt with how social media companies do with their users data and how they utilize that information. A member of our team went down the path that looked into the amount of digital data that we have stored in these hospital databases. The amount of information these hospitals have that deal with our personal information and physical health can have a major effect on us if that data and information gets breached or is stolen. Another of our fine writers went down the track that looked into how data collection is being collected through platforms such as Facebook and Google. And how these power hungry companies are basically using our personal information and data to advertise it right back to us, putting us in an endless cycle. Lastly our final writer went down the route that focuses on how Microsoft is dealing with data collecting and how they are trying to implement into Windows 10 and 11 new features that users can use to disable from their setting in order to minimize the way your data gets collected. As we each individually did our research we were also tasked with looking for if there is a resolution to this crisis we are dealing with. As we did our research we all were getting similar information when it came to coming up with a solution. We all saw how there is no permanent solution to this situation. What each of us were able to find was steps we can take to minimize our digital footprint.

Jerson Vargas

In conclusion, Based on what we have found within the results, our story tells us that there is no real way to solve or stop companies from stealing our data due to the fact that it is part of the monopoly of how companies make money and sell targeted ads to users, etc. Most big companies , such as Google, Microsoft, sell our data to companies based on what we search, watch and interact with on the internet every second of the day. Our privacy is one of the very most important aspects of our lives and what we do on a daily basis. When we use technology for our daily interactions, we need to make sure our privacy is not being stolen as least as possible from big companies. This can go from our own physical health, to what we watch and

lastly, what we purchase for ourselves. Little interactions like the examples said to help improve our life by using these technologies causes the companies to track, and give targeted ads based on the algorithms chosen.

RECOMMENDATIONS

Djeneba Bah

After doing this research, I have realized that there's no permanent solution for companies from collecting our personal data. However one can minimize to which extent they access one's personal data. A recommendation that I saw highly throughout my research is if you are a windows user, configure your PC as frequently as possible. Also disable some features in order to protect your privacy to the maximum. These alternatives deal with your local content and the ways in which it could track or collect your data online. Our point is not to alarm you or push you to deactivate everything, but to give you all the necessary information so that you can decide how far you want to expose yourself.

Jerson Vargas

Some things we should do to prevent our data from being stolen less are using different kinds of browsers that does not deal with stealing our information, for example DuckDuckGO. DuckDuckGO is a free to use browsing tool that does not allow your information to be stolen when using the tools needed. Also using tools such as a VPN which is a virtual private network. Which can then help lead us to not having our ip stolen from companies and potential hackers because we are connected to another machine with the VPN in another location. Another way to have your data least stolen is by using a virtual machine. Virtual Machines are usually used for big projects such as creating software for another operating system or testing the limits of an operating system you're using for the machine. Although Virtual Machines do not hide your IP address, It can prevent hackers from entering your main system and utterly destroying and taking over your PC.

References

Sengelmann, M. (2020). An Overview of Reverse Engineering and A Security Analysis of TikTok.

Stachl, C., Boyd, R. L., Horstmann, K. T., Khambatta, P., Matz, S. C., & Harari, G. M. (2021). Computational personality assessment. *Personality Science*, *2*, 1-22.

Burger-Lenehan, B., Weinberg, G., & duck, D. the. (n.d.). Spread privacy. Spread Privacy. Retrieved May 2, 2022, from https://spreadprivacy.com/

Are You Being Watched? What you need to know about targeted advertising. (2017). *Scholastic Scope*, 15.

Brandon, J. (2020, October 14). *How does a VPN protect your privacy and anonymity?* Tom's Guide.https://www.tomsguide.com/features/how-does-a-vpn-protect-your-privacy-and-anonymity

HACHMAN, M. (2015). The price of free: how Apple, Facebook, Microsoft, and Google sell you to advertisers. *PCWorld*, *33*(11), 51–59.

Wilbanks, J. T., & Topol, E. J. (2016, July 20). *Stop the privatization of Health Data*. Nature News. Retrieved May 9, 2022, from https://www.nature.com/articles/535345a

Nahdy, A. (2020, November 24). How to stop data collection by Microsoft on Windows 10. Retrieved May 3, 2022, from https://net2.com/how-to-stop-data-collection-by-microsoft-on-windows-10/

Whitelaw, S., Mamas, M. A., Topol, E., & Spall, H. G. C. V. (2020, June 29). *Applications of digital technology in COVID-19 pandemic planning and response*. The Lancet Digital Health. Retrieved May 9, 2022, from https://www.sciencedirect.com/science/article/pii/S2589750020301424