Introduction

As the second decade of the twentieth century nears to an end, technological developments have been at the center of our lives more than ever. As much as these developments can benefit our lives by making everyday actions much easier, it comes with its negative sides as well. It is a fact that our main form of communication is via social media sites and just like all the technological developments; it has its cons as much as it has its pros. Just a few generations ago, private messages were written by hand as a letter, and were mailed to the desired destination. Just a simple message could take days to reach its receiver. Nowadays; with social media sites, the time has been reduced to mere seconds. However; as previously mentioned, this convenience comes with a cost and this cost is mainly in the form of the loss of privacy. Personal space has shrunk so much that it is nearly non-existent at this point. Every time we register to a new social media site, we sign an agreement without even taking a look at it. This gives the companies a legal freedom of adding clauses that might go against the user’s personal space and private data. The biggest controversy regarding this issue has been the recent event surrounding Facebook and the company’s CEO Mark Zuckerberg. This issue along with some others will be further elaborated in the upcoming sections of this report.

Definition of Key Terms

Social Media

Websites and applications that allow users to create profiles and/or post content online for the viewing of other people usually referred to as “followers” and create a medium for everyday communication between individuals and/or groups.

Most popular social media sites include Facebook, WhatsApp, Tumblr, Instagram, Twitter, Snapchat, and many more.

Privacy

An individual’s “safe space” where no outside influence can disturb their thoughts, beliefs, ideas, etc.

Personal Data

A set of information that belongs to an individual
Internet Cookies

A pack of data sent by an Internet server to a browser, which is returned by the browser each time it subsequently accesses the same server, used to identify the user or track their access to the server.¹

Terms of Service

Also referred to as terms of use and terms of condition, these are legal disclaimers and agreements that users must abide by in order to use the service that is being provided.

These agreements are usually abused by companies by including clauses that may hurt the user as most users agree to these documents without any careful consideration.

Subpoena

It is a legal order for a person to attend a court.

Background Information

The Facebook-Cambridge Analytica Event

In March of 2018, social media giant Facebook and its CEO Mark Zuckerberg were the center of attention in the media for all the wrong reasons. When accusations stating that Facebook sold private data of millions of its users to political consulting firm Cambridge Analytica came out to be true, a huge legal process started. This resulted in Zuckerberg testifying in front of the United States Congress.

Afterwards, Zuckerberg gave many apologies and promised that there would be numerous changes implemented to Facebook. One of these changes that was implemented was suspending tens of thousands of applications after an investigation regarding data sharing. The reason behind these suspensions was that these applications made personal information of Facebook users public without the consent or notification of Facebook. The social media also sued many developers for not cooperating with them during the investigation and/or not complying by their restrictions regarding user safety/privacy. Some other notable promises by Facebook regarding the issue were:

- Informing users who were affected by this mishap.
- Making privacy setting more user friendly.
- Making access to personal data by applications tougher.
- Ending some of the targeted ads in the site.
The Apple- Federal Bureau of Investigation (FBI) Issue

Back in 2016, Apple CEO Tim Cook made a controversial decision to not cooperate with FBI after the Bureau's director at the time James Comey's order to unlock an iPhone used by a terrorist in an attack in San Bernardino, Syed Farook. The CEO stated that the refusal of this order was not because the company was aiding terrorism, but instead was a defence of civil liberties. He also added that this would set a “dangerous precedent for everyone’s civil liberties,” The company also stated that they were capable of developing such technologies which would enable them access an iPhone’s passcode, however this would be extremely dangerous as hackers and cybercriminals would attack this technology in order to gain access to it. Cook concluded his company’s stance by saying: “The only way to guarantee such a powerful tool isn’t abused and doesn’t fall into the wrong hands is to never create it.”

How Internet Cookies Work

The main tool used online to share information are cookies. They are packs of information gathered by web browsers which are then given to websites especially to give targeted advertisements to the users. For example, an online clothing store will use cookies in order to see what types of clothes a user usually browses. If the user views men’s sportswear, then the next time they visit the website, there might be some sort of a list with best men’s sportswear under a certain price point. So basically, a cookie can be best described as a personalized advertisement. The best way to make sure that the user is not at danger with these cookies, a website’s privacy policy and/or terms of agreement must always be checked.

How Can Social Media Companies Share Personal Information?

The worst part of this issue is that most acts committed by these companies may seem illegal, but are perfectly in order because of the loopholes they create for themselves in their terms of agreements. As previously mentioned, because majority of users agree to these terms without reading them, they miss out on crucial specifications as to what the companies are allowed to do. This is why the governments are supposed to interfere with this issue as most of these documents are nowhere near being user-friendly. Websites use internet cookies in order to access and share personal information of its users. In its core, cookies are pretty harmless as companies use them to gain financial advantages which is perfectly fine. Nearly every social media site is free to use and therefore, the companies’ main source of finance is via ads and cookies become extremely important in this case as they are much more beneficial for the advertiser because they are specifically tailored to the user. However, if the information gathered by cookies are used for purposes beyond advertising, such as supplying this information to a political consulting firm in order to gather classified information regarding an upcoming election is highly illegal and immoral.
Furthermore, another aspect of this issue that makes it much more complicated is the intervention of a third party. This makes the data exchange much harder to spot as it doesn’t stay in one place forever and is much more dangerous for the user as the third party that acquires the information directly from the company then can also share it with another party and this could go on and on, creating a web of information being shared thousands of times. The creation of this web will be extremely dangerous for the user as their personal information can get in the hands of anyone that is willing to gather this data for any kind of usage. This is how people get random text messages from companies they have never purchased an item from.

Major Countries and Organizations Involved

United States of America

As nearly all social media companies are based in the US, they hold a huge importance in this issue. Most recently, the US congress called the CEO of Facebook, Mark Zuckerberg for a testimony following his company’s scandal with Cambridge Analytica. Furthermore, there are many laws regarding internet use and personal information in the US. Some of the most notable ones are:

Electronic Communications Privacy Act (ECPA)

This law was passed back in 1986 and is highly controversial. It states that the government can access any personal data such as personal messages, emails, social media activity, GPS location, etc. with a subpoena. Furthermore, if the targeted information is older than 180 days, then the government doesn’t need any kind of warrant.

Children’s Online Privacy Protection Act (COPPA)

This law was implemented in 2000 and is the first US privacy law regarding the internet. It was written in order to specifically protect the information of children under the age of 13 on the internet and works together with the Federal Trade Commission (FTC).

China
When it comes to the internet, it is a known fact that China usually has unknown policies and very strict censorship laws. Very commonly accessed international websites such as YouTube, Twitter, Facebook, and Wikipedia are all blocked in the country. However, this doesn’t mean that they don’t have any form of laws regarding the protection of users’ personal information online. Very recently, in September 2019, there was a public outrage following a privacy issue surrounding the social media site Zao. Users were shocked and terrified when they found out that the application was allowed to use their created images and/or videos for free. After this outrage, the company stated that they will not be using any personal images and/or videos of their users. Furthermore, the Chinese public is starting to notice their rights and their personal space online and are standing up against some of the biggest companies in the world such as Alibaba in order to make sure that their private information is safe. In June 2019, the Cyberspace Administration of China (CAC) issued the Data Protection Regulatory Guideline which stated regulations and restrictions for online companies aiming to achieve a safe platform for their millions of users.

Russia

Perhaps the biggest issue regarding Russia and online privacy is the demand by the Russian government for all internet companies to make all online data “localized” which basically means that the government must be able to easily access this pool of information when they need to do so. Furthermore, the Russian government also passed a bill that imposes heavy fines on any companies that fail to meet the standards that have been set.

European Union (EU)

The EU is very strict when it comes to protecting the private information of its citizens. All companies that are providing service in EU countries are obliged to follow the rules and regulations set by the Union no matter the country of origin of the company. First of all, a legally binding agreement is mandatory for all internet companies that work with personal data of its users as the lack of such a document will result in any form of data collection to be deemed as illegal and will result in huge amounts of fines to be set on the company. These restrictions are known as the EU General Data Protection Regulation (GDPR).

Organisation for Economic Cooperation & Development (OECD)
This organization lets its 36 members to share data and information regarding the issue of public privacy and has come up with initiatives such as, “2007 Recommendations on Cross-Board Cooperation”, “2011 Report on the Implementation of the Recommendations”, “OECD Recommendation & Guidance on Electronic Authentication”, and many more.

Electronic Privacy Information Center (EPIC)

Established in 1994, this Non-Governmental Organization (NGO) works in order to secure privacy of the public. They conduct policy researches and provide campaigns in order to raise awareness on the issue and educate the people.

Timeline of Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 31st, 1974</td>
<td>US Federal Privacy Act is implemented.</td>
</tr>
<tr>
<td>1986</td>
<td>ECPA is implemented.</td>
</tr>
<tr>
<td>1994</td>
<td>EPIC is established.</td>
</tr>
<tr>
<td>April 21st, 2000</td>
<td>COPPA is implemented.</td>
</tr>
<tr>
<td>2007</td>
<td>OECD report titled “Recommendations on Cross-Board Cooperation” is published.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Facebook-Cambridge Analytica scandal occurs.</td>
</tr>
<tr>
<td>April 11th, 2018</td>
<td>Mark Zuckerberg, CEO of Facebook testifies before the US Congress.</td>
</tr>
<tr>
<td>May 25th, 2018</td>
<td>GDPR is implemented.</td>
</tr>
<tr>
<td>June 2019</td>
<td>Data Protection Regulatory Guideline is implemented in China.</td>
</tr>
</tbody>
</table>
Relevant UN Treaties and Events

As this issue is quite new in the world stage, the UN is still yet to debate and/or pass a resolution on it. However, as this issue and the concern regarding it is continuing to grow, the UN definitely needs to address it. However, there are some other documents and/or events outside the UN that would be highly beneficial during the research of this topic. These are:

- **Cross-Border Cooperation in the Enforcement of Privacy Laws**  

  This is an initiative by the OECD member states in order to have a better framework both domestically and internationally in order to protect privacy. It includes a commitment by member states’ governments in order to have better laws regarding the issue and provide assistance for fellow member states’ governments. This initiative can be deemed as an amendment to 1980 OECD Privacy Guidelines.

- **Framework & Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**  

  This is also a recommendation by the OECD member states for governments to take necessary steps in order to achieve a safe environment for personal information. Furthermore, one of the recommendations state that although governments must take precautions to secure a safe space, these requirements must not interfere and/or create burdens for any beneficial data flow.

- **Digital Identity Management & Electronic Authentication**  

  This is a report which gathers numerous works done by OECD from 2007-2011 in order to create a better understanding about the very complex question of digital identity to governments all around the world.
Previous Attempts to solve the Issue

As previously mentioned, the UN has still not made an attempt to solve this issue. However, governments all around the world are closely monitoring websites in order to prevent any mishaps to occur. There are many laws passed in most countries' respective constitution regarding this issue. Furthermore, these laws are still being amended as the issue is ever-changing with new technological developments and new social media sites.

Perhaps the biggest actors in the fight against social media companies harvesting personal data of its users' after the governments are the users themselves. Most of these scandals occur with public outrage as mentioned in previous sections of this report. Furthermore, there are many organizations working alongside and for the people in order to educate them regarding the issue. This way the users now their rights and their freedom while using these services that are being provided to them. The fact that the public is educated on the topic more than ever results in companies failing to perform the unlawful acts of a few years ago.

Possible Solutions

As the issue starts with the term “developing an international framework”, all resolutions on this issue must include clauses that aim to create international laws which will protect users’ private information with restrictions on what these companies can and cannot do and include in their terms and conditions. An example for these restrictions can be a word or page limit to these terms and conditions which will make them much more user-friendly and therefore can decrease users being victimized.

Another possible solution is the creation of an international organization after the implementation of the aforementioned international law that will closely monitor these social media sites to detect any unlawful act that might be committed and protect the users. Furthermore, these organizations can require social media sites to report regularly to see if there are any issues surrounding the question at hand. Moreover, in order to prevent any bias that might occur, these organizations can work with and/or for a broader international organization such as the UN.

A specific regulation for all social media sites can be implemented where they will be obliged to delete any and all personal information of a user once they delete their account and/or delete the
application from their device in order to secure the information after the user is no longer active on the website.

**Bibliography**


Appendix or Appendices