Forum: General Assembly Sixth Committee

Issue: Legal measures to protect the use of personal data by social media companies

Student Officer: Akhil Venkatesh

Position: Deputy Chair Sixth Committee

Nota bene: Seeing as the issue is one that continues to persist and encounters changes quite rapidly, this research report will cover only the data and information published before August 3, 2019. News and occurrences after the aforementioned date will not be incorporated into the report, but will, of course, be highly relevant to debate during the time of the conference in November.

Introduction

As the world continues to digitize at a rapid rate, with technological breakthroughs and scientific discoveries at every corner - greatening the potential and power of ingenious inventions and innovations, adaptation becomes key, in an ever-changing environment. Yet, the adaptation and integration that is sought, is not as seamless as one may think. Social media - a phenomenon which began in 1997, with the app Six Degrees has now revolutionized the way people act, think, and interact with one another. From apps such as Linkedin in the early 2000s, to Youtube in 2005, all the way to Facebook and Twitter in 2006, and most recently - Instagram and Snapchat, in 2010 and 2011 respectively. Social media has truly benefited humans in ways that may have been thought of as heresy in the past. It allows for interactions between not only friends and family members across the globe, but also complete strangers. Social media was designed to connect people with one another, enabling users with a platform of self-expression and a source of information. Although all of the aforementioned benefits still exist, with them, come a set of dangers to keep in mind.

In the current day and age (known as the Digital Era), data is highly powerful. Data is used and collected every day - whether it is asking a question or poll on Instagram, or viewing someone’s story. Data drives corporate businesses, it empowers them with important information relating to their consumers. This, quite obviously means that data lends itself to both good causes and bad ones. Data has the potential to be manipulated and can be used to garner greater profits. As social media usage is becoming more and more prevalent, so are the data collection methods and various search algorithms used by companies. The popular quote “With great power comes great responsibility,” is an epitome of
the data gathering systems used nowadays, especially by social media companies. The truth of the matter is that social media companies have access to a lot more information than their users may think. Hence, it is important to tread carefully and think before a person shares, or messages an individual or group. For everything that is old, may become new in the span of a mere second.

**Definition of Key Terms**

**Social Media**

Social media is defined in the Merriam-Webster dictionary as forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos). This term will be highly prevalent throughout this research report, being the main topic of discussion.

**Personal Data**

According to the European Commission, personal data refers to any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

The General Data Protection Regulation (GDPR) protects personal data regardless of the technology used for processing that data – it is technology-neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn’t matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data include:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.
Privacy

Under the Human Rights Council Resolution on the promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development (A/HRC/23/40), privacy is defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. Under the Universal Declaration of Human Rights (UDHR), Article 12, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used. Privacy, in this day and age, is of most importance. It is key to trust between consumers and businesses. This is also the reason why various data protection and privacy laws have been enacted ever since recent scandals and controversies.

Cookies

Cookies are small amounts of data generated by a website, which are then saved by your web browser. Their purpose is to remember information about you. While cookies serve many functions, their most common purpose is to store login information for a specific site. Some sites will save both your username and password in a cookie, while others, only your username. Cookies are also used to store user preferences for a particular site. For example, a search engine may store your search settings in a cookie. A news website may use a cookie to save a custom text size you have selected for viewing news articles. If a website or social media app needs to store a lot of personal information, it may use a cookie to remember who you are - loading the information from the web server. This method, widely known as “server side” storage is often used when you create an account on a website or through an application.

![Cookies Pop-up Example](image)

**Figure 1:** Cookies Pop-up Example (jQueryScript)

Data Mining
Data mining is known as the process of analyzing hidden patterns of data according to different perspectives for categorization into useful information. This information is then collected and assembled in common areas such as data warehouses for efficient analysis. These then facilitate business decision making and other information requirements to ultimately cut costs and increase revenue. Social media companies use data mining technologies to learn more about their consumers and appeal to their needs in a much more beneficial way - all, of course, in the end to reap greater profits. If the social media companies themselves do not do so, they often sell the data off to other companies, who would then use it for advertising purposes.

Social Data

Social data refers to the information that social media users publicly share. This is inclusive of metadata such as the user’s location, language spoken, biographical data, and/or shared links. Other examples are posts, stories, and messages made on the platform. Social data is often used to help businesses advertise and market to targeted users who would be more likely to be interested in their products. Facebook for Business and Twitter Ads are two such programs helping advertisers use social data.

Targeted Advertising/Ad Targeting

Targeted advertising/ad targeting is an advertising technique where advertisements are placed in specific areas of the screen to increase visibility or to give tailored ads based on the user’s past behaviors and preferences. Targeted ads are meant to reach certain customers based on demographics, psychographics, behavior and other second-order activities that are learned usually through data exhaust produced by the users themselves. In some cases, ads are targeted based on your current browser page, using related searches and/or keywords.

Figure 2: Ad Targeting Example (Aylien Blog)
Background Information

The Prevalence of Social Media

Although social media had its humble beginnings in the 1990s to early 2000s, with apps such as Six Degrees and Linkedin, its popularity amongst the youth, and surprisingly the adult population, has skyrocketed ever since. Social media has now become an integral part of our daily routines. If 20 years ago, it was unconventional to be checking your phone every morning, it no longer is. Social media has become the pinnacle of information, interactions, and sharing. The saying “information is at the tip of our fingers,” could not be more fitting. With over 3.256 billion mobile social media users in 2019, it is safe to say that social media is definitely currently trending. A 2018 report from GlobalWebIndex found that on average, social media users would spend approximately 2 hours and 22 minutes online each day globally - with teens clocking in at about 3 hours. The data goes to show the important role that social media plays in a human being’s life nowadays.

Figure 3: Digital Usage of Social Media Infographic (Hootsuite)

Social media giants such as Facebook, Tencent, and Google essentially dominate the market. Facebook owns both Whatsapp and Instagram, while Google owns Youtube and Tencent owns WeChat. Apps such as WeChat can essentially be used for anything - whether it be shopping online, banking, browsing the web.

Social Media Companies and Their Deal With Data
Why Social Media Companies Collect and Use Data

However, with all of the obvious benefits that can be seen, one may question how social media companies do it. Delving deeper into what data is collected and how it is processed in order to ensure seamless integration with the various resources available to us on these apps may provide an answer. Social media companies firstly collect basic data (usually when you register an account on the platform): name, gender, date of birth, email or mobile number. The next step after this, is to collect personal data, to target ads to that user: every single ad the user clicks on, any additional personal information added to the profile (schools, hometown, current city, alumni associations, other social networks, employment, political clubs, groups), every IP address that users have used when logging into their account, every friend in their network/social circle, including ones that have been unfriended, deleted or removed, the user’s activity - all of it (when you liked a page, you were tagged, status changes, searches, everything). Seeing as companies collect a lot more data about us than meets the eye, there is no doubt in the fact that they also often sell or use it for ad targeting. What often occurs after the collection stage, is that they sell and redistribute the data to advertising agencies or third parties. These third parties will then target specific users based on the data in an effort to garner greater profits through targeted advertising.

The Importance of Personal Data Privacy within Social Media

As a growing number of citizens are now becoming aware of these methods of data collection used by social media companies - it begs the question of why privacy is important. Although there are various privacy option levels offered by the social media companies themselves, to protect personal data from being seen by complete strangers (private vs. public profiles, hiding various elements within the “about me” section), the social media companies themselves still have access to heaps of information about their users. Whilst users may think that they are “anonymous”, it is safe to say, for the most part, that they are traceable using information such as IP addresses, which are unique to each and every user based on their connection point (e.g Wifi). Yet, even with this tool, there is only so much that can be done by social media companies themselves - at the end of the day, it is all user-oriented. Unfortunately though, the default settings on sites such as Facebook do not seem to offer sufficient privacy. With many users unaware of privacy settings, sensitive personal information is often released to complete strangers unintentionally. However, even if this may be a concern to users, the real concern appears to be with the social media companies themselves. This is because of third party involvement within apps such as Facebook, and the constant data collection methods used by them. With the plethora of data collection methods available to social media companies, the ways in which they dispose of them come into question. Quite often, the data ends up being sold
off, or stolen due to data breaches. This in turn, makes social media usage somewhat less private, and more intrusive to one's personal privacy online.

**Figure 4:** In-depth infographic on data collection and usage by social media giants (Baynote)
Social media companies have been under fire since early 2018 after tons of data scandals and leaks occurred. Cases of hacking have been taking place for a long time, but in these instances, the social media companies were colluding with third parties, which is what makes it all the more different and surprising.

**The Cambridge Analytica Scandal**

A widely known data scandal was that concerning Facebook and a political consulting firm, Cambridge Analytica. Cambridge Analytica had been collecting data from Facebook users who had agreed to take a psychology questionnaire. Not only could Cambridge Analytica access the data of the person who took the survey, they could also access all of the data of that person’s Facebook friends. The data in question was being used in an attempt to sway people’s beliefs in hopes that they would vote for a certain politician. The use of an Application Programming Interface (API) for data collection can be a focal point of the privacy conversation. While the data can be anonymous, the difficulty is understanding when it becomes an invasion of privacy. Personal information can be collected in mass, but the debate over whether it breaches personal privacy is due to the inability to match this information with specific people. There have however been some concerns with API because of the recent scandal between Facebook and Cambridge Analytica. The reason being, Facebook allowed a third-party developer to engineer an application for the sole purpose of gathering data. The developer was able to exploit a loophole to gather information on not only people who used the app but all their friends - without them knowing.

**The Quora Data Breach**

Although the Cambridge Analytica scandal was quite heavily covered by the media, a data breach that went almost unrecognized was that of Quora’s. Quora, a question-answer website had its data compromised in December of 2018. This security breach affected more than 100 million users. Users’ account information, including names, email addresses, encrypted passwords and data imported from linked networks when authorised by users may have been compromised, according to CEO, Adam D’Angelo.

**Repercussions on Everyday Users**

After the scandal, news spread quite quickly. This, in turn, caused outrage within the user population. As an effect, people began to trust social media networks less, and social media companies saw a decline in users. Many began to learn about privacy and data protection methods. Looking in retrospect, the Cambridge Analytica scandal provided people with a warning in regards to privacy, and a message to social media companies to tighten security measures and cater to the people before seeking out greater profits. From the European Union rolling out the General Data Protection Regulation (GDPR)
to governments enacting laws targeted at social media companies, all the way to instances such as a Select Committee on Online Falsehoods being formed to counteract and reveal information about fake news. Overall, general awareness of privacy, data protection and their relation to social media companies increased, resulting in a more cautious mindset.

Major Countries and Organizations Involved

Social Media Companies

Social media companies play quite an important role in regards to the matter, as they are the ones that dictate how user data is collected, where it is stored, and to whom it is sold or given to. As can be seen in the Facebook-Cambridge Analytica scandal, oftentimes, companies’ best interests in profit-making may take over the objective of user privacy and data protection. This, in turn, permits space and potential for loopholes to be taken advantage of. Due to the fact that many social media platforms run on an API - which in itself is quite new to the growing population, there is great potential for third parties to gain access to unwarranted information, such as can be seen in the aforementioned case. Yet, Facebook is not alone in its data ventures. Google, Twitter, all kinds of online platforms, LinkedIn, Instagram (owned by Facebook), Snapchat, and many more all have access to highly sensitive private data, which is stored on their servers and could be stolen anytime now. Some of them were victims of data breaches, like LinkedIn, and Snapchat. More than 360 million MySpace user credentials surfaced online. Most social networks use poor security measures and aren’t even able to recognize all of the fake accounts they have on their platforms. Google uses all kinds of data from their users, and numerous apps on Android and on the web also have access to the data (just check out all of the permissions you gave to various apps installed on your smartphone). The general stance of social media companies is that they want user data, no matter the cost. This is due to the fact that data drives and powers their business. Without the data, they wouldn't be able to draw in customers (usually advertising agencies). Without ads, they would essentially be making no money at all.

The European Union (EU)

Although the EU has held various talks and attempted to take action in regards to data protection in the past, they recently grabbed the attention of people across the globe after the establishment and implementation of the General Data Protection Regulation (GDPR) on May 25, 2018. The GDPR provides a set of data protection rules for all companies operating within the EU - wherever they are based. From banking to healthcare (meaning social media companies too).

The United States of America (USA)
Home to various social media giants, the US has a major role to play in the issue. When the Cambridge Analytica scandal occurred, the US Congress had Facebook’s CEO, Mark Zuckerberg, testify before their senators. There are several federal laws that touch on social media privacy concerns, including The Communications Decency Act (CDA) and The Children’s Online Privacy Protection Act (COPPA). But, many other efforts have been made to enact federal legislation to better address social media protections. Unfortunately, no national comprehensive social media privacy laws exist yet; there is no U.S. equivalent to the EU’s General Data Protection Regulation (GDPR).

Some states have taken measures to better protect social media privacy, with laws that usually fall into the following categories:

- Laws requiring implementation of security measures;
- Laws imposing liability and criminal punishment for hacking; and
- Laws requiring notification for data breaches.

For example, California law requires persons or businesses that conduct business in California to give consumers notice of a data breach in the "most expedient time possible."

**The People’s Republic of China (China)**

The People’s Republic of China has been known worldwide for its censorship laws and strict measures regarding user activity online. China sits in a quite interesting perspective. Various applications and social media platforms are banned in China. Youtube, Instagram, Facebook and Whatsapp are key examples of the social media platforms that have been blocked. In replacement, come Youku and WeChat. However, a quick look at WeChat will lead one to think - although the regulations set out against users are highly enforced, there are not many regulations set for the social media companies, of those that exist. Yet, seeing as many of the companies involved in data breaches have their sites blocked in China, one may be led to thinking that the Chinese government is actually protecting its users and ensuring personal data privacy through the blockage of these platforms. Paying with a smartphone using Alibaba-affiliated Alipay or Tencent’s WeChat Pay has become ubiquitous, while WeChat has become the default messaging app for both personal and business discussions. As a result, China’s tech giants have accrued huge amounts of information on their users, which some worry, could be used inappropriately.

It seems most Chinese are willing to give up details about their financial, personal and professional lives for the sake of convenience, but that may be changing as consumers become more aware of security issues and companies work to improve collection practices. In November of 2018, the
China Consumers Association released a report stating that 91 of 100 apps it surveyed may be suspected of excessive data collection.

The Republic of India (India)

India has maintained quite strong privacy rules throughout history. That of social media is no different. The strongest legal protection provided to personal information in India is through section 43A of the Information Technology Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 developed under the section. The provision requires a body corporate who 'receives, possesses, stores, deals, or handles' any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which they are held liable to compensate those affected. The Rules under section 43A contain various requirements and can be found here (not included due to space constraints)

Timeline of Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>Birth of the cookie: Netscape is credited with inventing the browser &quot;cookie,&quot; the innocently named little computer file that enables firms to build a profile of a user by recognizing and tracking his or her web surfing behavior.</td>
</tr>
<tr>
<td>1995</td>
<td>EU concerns - Against the backdrop of long-standing, pre-Internet concerns about privacy and the protection of personal data, the EU issues its first data protection directive regarding the processing of personal data and its free movement.</td>
</tr>
<tr>
<td>1997</td>
<td>Social networking website SixDegrees.com is created, which is said to be the first ever social media website.</td>
</tr>
<tr>
<td>2001</td>
<td>Six weeks after the Sept. 11 terrorist attacks, President George W. Bush signs the Patriot Act into law. The bill, which grants broad new surveillance powers to law enforcement and intelligence agencies, is designed &quot;to identify, to dismantle, to disrupt and to punish terrorists before they strike.&quot; After passing both the House and Senate by wide margins, the Patriot Act widens the scope of the Foreign Intelligence Surveillance Act, or FISA, and includes a variety of...</td>
</tr>
</tbody>
</table>
provisions that allow for expanded data collection and surveillance by government, as well as disclosure of electronic communications.

The Pentagon is revealed to be building "a computer system that could create a vast electronic dragnet, searching for personal information as part of the hunt for terrorists around the globe — including the United States." The system, known as "Total Information Awareness," is designed to use data mining techniques to find hidden patterns of activity from vast troves of Internet mail information, credit card and banking transactions, and government documents. Aside from concerns over its scope, the Orwellian ring to the program's name proves problematic. Within months of the initial headlines revealing its existence, it's changed to a less threatening moniker: "Terrorism Information Awareness."

In September 2006, Facebook, the popular social networking service, launches its new News Feed feature, which broadcasts changes members make to their Web profiles to the pages of others in their Facebook social networks. After an uproar, fueled by complaints about the invasiveness of the feature, Facebook quickly apologizes and lets users disable or modify it. A year later, Facebook again angers users with the introduction of Beacon, a program that sends news alerts to users' friends about which goods and services they purchased online. After widespread criticism and a class-action lawsuit, Beacon is shut down in late 2009.

Tens of thousands of Facebook users protest against terms of service changes that allow Facebook to use anything uploaded to the site at any time, even after users have deleted their profiles and left Facebook. After the backlash, the company reverts to its original policy and issues a statement of rights and responsibilities surrounding its relationship with users.

Google agrees to settle Federal Trade Commission charges that it used deceptive tactics and violated its own privacy promises to consumers when it
launched its social network Google Buzz in 2010. Google had received thousands of complaints from users who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers or competitors. The settlement calls for implementation of a comprehensive privacy program, and for regular, independent privacy audits for the next 20 years, marking the first time an FTC settlement order requires a company to implement a comprehensive privacy program to protect the privacy of consumers' information.

In January, Google announces it will integrate user data across its email, video, social-networking and other services. In a blog post, the company explains the plan will lead to "a beautifully simple, intuitive user experience across Google." "Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services," Google writes. "In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience."

Cambridge Analytica begins their illicit harvesting of personal data via Facebook's platform (through the form of surveys). In 2018, the scandal erupts - leaving millions in shock, and many, fearing for their own personal data privacy.

Relevant UN Treaties and Events

Although there are no specific resolutions or conventions in regards to personal data privacy on social media, there are a few on the right to privacy as a whole (which essentially constitute a few overlapping main ideas, calling for action from governments mainly, but also putting pressure on social media giants as a result):

- The Right to Privacy in the Digital Age, 18 December 2013 (A/RES/68/167)

Previous Attempts to Solve the Issue
Although there has not been substantial action taken against personal data usage by social media companies (especially due to the fact that the issue is still unfamiliar to many), there have been quite a few minor, short-term solutions to the matter.

**The European Union**

As mentioned previously, the European Union implemented the GDPR in May of 2018, and ever since, processes involving personal data have become more secure and safer. The GDPR also enforces that companies use the best security practices to ensure that there are fewer chances of data breaches and leaks occurring. With these stronger rules on data protection, people have more control over their personal data and businesses are able to benefit from a level playing field. This ensures that leaks and breaches in data are less likely to happen. The regulation covers even simple processes such as those of travel services.

**Social Media Companies Themselves**

Although various organizations have taken action and new legislation has been introduced, due to outrage from the international community regarding personal data privacy online - companies such as Facebook have been forced to rework their regulations and clearly communicate to users, the type of methods they use and how they collect user data. In the case of Facebook itself, it reviewed its terms of service earlier this year - in June, and decided to include a new statement on how it profits from targeted ads. Disclosures have been flooding in through social media apps since the various data breaches in the past decade. Now, companies’ main goal is to establish a sense of trust and transparency between themselves and their users.

**Governments**

Although social media companies and the European Union have taken action previously, it is up to the governments to enforce and regulate these companies on a day to day basis. Unfortunately, not all countries are actively participating in data protection on social media - but this is mostly due to the fact that they are already quite busy dealing with a more potent and volatile issue. Various countries have introduced legislation and formed conventions and resolutions targeted at the issue. Some have formed special committees to combat it.

**Possible Solutions**

**Changes in Data Collection Processes**
An obvious solution to the matter may be to get social media companies to simply apply changes in their data collection processes. Yet, to be quite frank, this solution is a last-resort. No social media company would change their data collection processes unless forced to. This is caused by massive earnings and the goal that companies have, to garner greater profits. If needed, however, the data that is collected by social media companies from users, could be changed.

**Further Government Regulation**

Another solution to improving social media privacy is to introduce strict regulations on the exact type of data that large technological corporations would be mandated to follow. However, since many such companies rely heavily on consumer’s personal data through its sale to advertising agencies, a crackdown on the type of data and its uses would be hard to execute. Nevertheless, such programs could potentially grant subsidies to minimize the loss of revenues, seeing that the majority of these corporations are headquartered in MEDCs. Further legislation and regulations formed by each individual government would allow for a more targeted approach per case. Social media companies would be forced to comply, or else, face blockage or removal.

**Enhanced Privacy Control Options for Users**

If social media companies are unwilling to amend their ways and move progressively - a step that they may agree to, would be a greater range of privacy options for users. Users, when joining, would be able to specify as to whether or not they would be fine with having their data collected. This would be similar to a disclosure on a social media app, except that the user would be able to choose as to whether or not to share their data with the company. This would reduce the amount of unhappy customers, and at the same time, increase transparency between governments and social media companies - serving well in the long-run for these businesses.

**Public Awareness**

A potential solution to this growing issue is to provide clearer and more simplified disclosures to users when using a service which would be undermining their privacy. While being maximally informed of the privacy risks, Carnegie Mellon University conducted research to find out whether that would be practical. It is estimated that it would take the average individual living in an MEDC over 76 work days to read all the privacy policies they absent-mindedly agree to, on a daily basis. Helping consumers better understand the privacy risks involved would help them make better decisions, while potentially staying more economically productive. Yet another solution that governments should potentially focus on is the sale and use of personal information. Although it is common that many governments collect personal data on their citizens for the purposes of national security and development, there may be only limited ways to encourage countries to reduce or end this practice altogether. Nevertheless, the focus can shift,
rather, to large corporations and their use and distribution of private information. Enforcing stricter regulations and audits on the ways that large corporations may use the personal information of their customers and outsource it to advertisement agencies. This may initially have a negative side-effect on the profitability and economic output of these corporations, but the long-term departure from an information-selling business model of companies would help attract more customers, and thus increases revenue streams.

**Bibliography**


“Cookie.” *Cookie Definition*, techterms.com/definition/cookie.


“The EU General Data Protection Regulation (GDPR) Is the Most Important Change in Data Privacy Regulation in 20 Years.” *EUGDPR Home Comments*, eugdpr.org/.


Appendix or Appendices

I.  https://eugdpr.org/

The European Union’s General Data Protection Regulation is an important point of debate regarding this issue, as it has changed the way in which companies that have offices in the EU have to respond to data privacy. This will give you a glimpse at how various nations now have to handle social media data privacy, and how it may affect the social media companies themselves.


Type of data that Facebook and other social media companies collect from you as a user.


Brief introduction to personal data by the European Commission (has useful links on data protection as a whole within the site as well).


An analysis into Data Protection and its priority level within companies.

An explanation of how big companies are able to collect customer data.