Forum: Special Conference 1 - Communications in a Globalised World

Issue: Handling of personal data by social media companies

Student Officer: Giao Giao Ma

Position: President

Introduction

Nowadays, social media companies keep record of all user activity. This not only includes whatever picture we give a thumbs up to or profiles we visit or follow, but also our location, telephone number, passwords, credit card number, contacts, among many other. What do these companies do with all this information? They often use it for publicity, taking into account the interests of each user and their location. It may seem harmless but up to what extent? This information could be useful for many other purposes, such as the infamous facebook "leak", which will be analysed later. The slightest mishandle of information could be used for unethical, immoral purposes, may these be political, or even terrorist.

How come the gathering of so much personal information can be so fragile and yet easy to obtain. It ought to be regulated. However, with social media being extended worldwide, every country has a different regulation to ir, or even none.

Moreover, how far does the handling of personal data by social media companies respect Article 12 of the Universal Declaration of Human Rights? Does each State regulate the use and protection companies give to the data they retrieve?

Definition of Key Terms

Personal data

"Personal data is 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." – European Commission

Social media

"Social media is a computer-based technology that facilitates the sharing of ideas and information and the building of virtual networks and communities. By design, social media is internet based and offers users easy electronic communication of personal

information and other content, such as videos and photos. Users engage with social media via computer, tablet or smartphone via web-based software or web application, often utilizing it for messaging.

Social media originated as a tool that people used to interact with friends and family but was later adopted by businesses that wanted to take advantage of a popular new communication method to reach out to customers. The power of social media is the ability to connect and share information with anyone on Earth (or multitudes of people) as long as they also use social media." – Investopedia

Data handling

"Data handling is the process of ensuring that research data is stored, archived or disposed off in a safe and secure manner during and after the conclusion of a research project. This includes the development of policies and procedures to manage data handled electronically as well as through non-electronic means.

Data handling is important in ensuring the integrity of research data since it addresses concerns related to confidentially, security, and preservation/retention of research data. Proper planning for data handling can also result in efficient and economical storage, retrieval, and disposal of data. In the case of data handled electronically, data integrity is a primary concern to ensure that recorded data is not altered, erased, lost or accessed by unauthorized users." – Office of Research Integrity

Automated Data Processing

"An Automated Data Processing is a technology that automatically processes data where technical devices like computers and communicating electronics are attached to gather, store and distribute data. The reason for Automated Data Processing is to process a large amount of information quickly with minimum human effort and also share with a selected audience. We can see Automated Data Processing applications for broadcast signals, weather advisories, and campus security updates. Automated Processing in computers are generally mutable and can be done through changes in infrastructure or organizational structure. In businesses, it mainly consists of integrated applications or restructuring of labor resources etc." – CIO whitepapers review

Right to Privacy

"The right of a person to be free from intrusion into or publicity concerning matters of a personal nature" – Merriam-Webster Dictionary

Article 12 of the Universal Declaration of Human Rights states "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."

We can agree that among one's matters of a personal nature, our personal data that we share with social media companies is included. Therefore it can be understood that social media companies have a responsibility when ensuring that the right to privacy of its users is not violated.

Background information

Legislation

International legislation

Up to date, the **General Data Protection Regulation**, enforced by the European Commission on 2018, has been the most successful yet obviously not completely efficient international legislation to be ratified on this issue, given the constant innovation in the areas of technology and communications. Its main objectives are "harmonize data privacy laws across Europe", "protect and empower all EU citizens data privacy", and "reshape the way organizations across the region approach data privacy." (eugdpr.org, 2018)

On the other hand, the **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** by the Council of Europe on 28 January 1981 in Strasbourg aimed towards the strengthening of data protection through, for example, the legal protection of individuals regarding the automatic processing of personal data related to them.

Russian Federation

Russia has a very particular legislation regarding the handling of personal data. To begin with, Russia is one of the ratifiers of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data on 2005, so the

history of data protection in this country is about 14 years old, which is not long. In 2014, Russia adopted personal data localisation rules, requiring all operators that collect and process personal data of Russian citizens to use databases located in Russia. This means that all foreign businesses are required to use local databases, which many believe excessive and convenient given that they need to transfer the data to their own databases afterwards. Those sites which do not comply with the local data processing have the option of being blocked. This can be interpreted as a security measure from the Russian government towards its citizens, such as the new legislation requiring personal data to be retained on Russian territory for at least six months as a counter-terrorism rule.

United States of America

The **United States of America** is known for being a fierce defender of individual's privacy, as can be seen in its 1974 **Privacy Act**. However, one's privacy in social media can be easily disrupted as someone posts a picture of a friend without his consent, or even a stranger. Maybe a post in some party after a shot or two can be damaging towards this individual's reputation and image, therefore making it hard for him to get a job. Regarding data, have you noticed how you can be tagged in any post without your initial permission? Sure, you can obviously untag yourself but your name has already been shared with everyone who has seen the post, regardless its content. The First Amendment of the US grants free speech, but up to what extent does free speech not violate the right of privacy of others?

In 1998, the Congress passed the **Children's Online Privacy Protection Act** (COPPA), amended in 2012. This Rule is meant to give the parents or guardian of the young child control over what information is shared in media concerning this child. Third parties are also aware that the data they are being allowed to use belong to children under 13.

Countries with no legislation

Many countries lack legislation to regulate the managing of personal data by companies in general. Plus, there is no international legislation applicable to all countries in this case. Many countries do have data protection policies but some are not considered adequate by the EU.

Universal Declaration of Human Rights

"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." – Universal Declaration of Human Rights, Article 12.

This article of the Universal Declaration of Human Rights expresses the right to privacy previously defined. It also expresses that the law should protect the individuals against such. However, many countries lack of efficient legislation to protect its population as this article suggests.

Companies' terms and conditions

Each social media has a set of terms and conditions the user has to accept to be able to join it. However, most people do not read these and still accept. This can cause many issues regarding personal data. For example, during the infamous Facebook scandal which will be talked about later, it may come to mind whether most people even knew it was against what they had agreed on.

This can become a problem if the user is subject to harm in this media but is unable to complain given that he acceded to this harm when he accepted the page's terms and conditions without reading them carefully.

People should be aware that in any social media they are giving access to personal data such as names, address, phone number, e-mail, even credit card number, among others. These are usually used for publicity, so as to show you propaganda you might be interested in, which is harmless. However, it might not be as harmless if this social media company sells private data to be used for reasons you may objectify but the terms and conditions specified that the company did not take responsibility for third party data users.

In conclusion, it would be better if people read the terms and conditions before accepting and joining a social network. It may seem like a tedious, unnecessary formality, but users would take responsibility for what is being done with their personal data.

Insecurity

Black market of data

All sort of data surfs the black market, specially personal data such as credit card numbers and passwords, social security numbers and even social media accounts. How do hackers use social media to obtain this information? Large social networks are not effective when detecting bots or fake accounts, or even social media companies themselves sell their users' data.

Cybercrime

Personal data can be used for cybercrime, for example cyberterrorism. In our social profiles we often express our fears or most sensitive aspects under the camouflage of anonymity. Yet, terrorist groups may use this information to target a certain public and spreading fear through social media. An individual's name is not important when one is managing crowds. On the other hand, criminals may target certain people based on their social media profile. Now the option of keeping a private profile is available, however a description and name is given in Facebook and Instagram, for example. Otherwise, with the power of twenty-first century influencers, accounts with many followers are also target given the accounts' abilities to move crowds.

It is certain that with the development of technology and communications, laws and regulations must evolve and apply so as to keep an order and security among the users.

Facebook scandal

Cambridge Analytica is a political consulting firm which worked for the Donald Trump campaign in 2016 by harvesting raw data from more than 50 million web users in order to conduct their behaviour into supporting the candidate aforementioned.

How did this happen? Facebook allowed the harvesting of its users data through a quiz app called This Is Your Digital Life. Not only did it collect the data of those who took the quiz, but also the data of their friends, showing a huge loophole in Facebook's application programming interface. This was against Facebook's terms and conditions, however Cambridge Analytica sold the data anyways. Allegedly, Facebook was aware of the data being harvested but denied it. Furthermore, Cambridge Analytica claimed it was unaware of how the data had been harvested and deleted it when it found out. It was a scandal also

because the personal data was used in order to influence voters, which is both unethical and illicit.

It should also be taken into consideration what a huge market Facebook implies. Just think how many social media companies use Facebook accounts as an option to log in, save a game or add friends. How many times has the option “connect to Facebook” been seen in games? These third party applications are able to access your whole list of contacts with just one click. How hard can it be to access the rest of the data?

After the scandal, Facebook has limited the access to information for third parties. But, would it really have if no allegations had taken place? How much can the social media be trusted when handling personal data when it comes to profit?

Major Countries and Organizations Involved

United States of America

The United States of America, being a federal State, has no general law that protects data but rather regional laws. However, each Congressional term brings proposals to standardise laws at a federal level. Therefore, there are many state laws and federal regulations which contradict each other. In addition, there are many regulatory guidelines developed by governmental agencies and industry groups which do not have force of law but rather contribute to a state of “self-regulation” that each company decides to follow. These guidelines include accountability and enforcement components.

So it is understood that the situation is hard to control inside the country, despite there being a clear position in favour of data protection and user satisfaction.

As many worldwide social media companies have their servers in the United States, this country’s legislation is most influential in social media companies (e.g. Facebook, Twitter, Snapchat, Linkedin) and remains invariable compared to other countries legislations.

Russian Federation

The Russian Federation, as aforementioned, is a special case when talking about social media data handling regulations. It does have legislation which regulates the circulation and processing of personal user data, which is great, however it may not be the

most conventional as it requires that all data is handled in servers inside the country before transferring it to outside servers.

People's Republic of China

China has a particular network when talking about the internet, since the data and services that enter and exit the country's network are highly regulated by the well known firewall. However, it was not until 2017 that China put up its own data protection legislation for data handling companies and set some regulations for them to comply with when handling user data.

United Kingdom

United Kingdom updated its own legislation on the protection of data complementing with the EU GDPR with the 2018 Data Protection Act. Ever since its first Data Protection Act in 1984, UK has worked to adapt the protection of data to the fast advances in technology (Matt Burgess. *What is the GDPR? The summary guide to GDPR compliance in the UK*), being this of last year the last update to data protection regulations.

United Nations Conference on Trade and Development (UNCTAD)

Being the Internet the modern and growing means of trade, the UNTAD finds focus on helping trade grow, and to do so they need users to trust the Internet and the media. If privacy and safety is not provided to users, development in the areas of trade will not be possible. Therefore, it is needed that everything works correctly for the global economy to further develop.

United Nations Global Pulse

Global Pulse is a flagship innovation initiative of the United Nations Secretary-General on big data. Its vision is a future in which big data is harnessed safely and responsibly as a public good. Its mission is to accelerate discovery, development and scaled adoption of big data innovation for sustainable development and humanitarian action. (unglobalpulse.org)

The Internet Society

The Internet Society (ISOC) is a non-profit organization dedicated to ensuring the open development, evolution and use of the Internet. (Internet Society, 2018)

European Union

The General Data Protection Regulation 2016/679 is a regulation in the EU law which protects the rights of its citizens regarding the security of their personal data and privacy.

African Union (AU)

In 2014, the AU members adopted the African Union Convention on Cyber Security and Personal Data Protection and to facilitate the implementation of the Convention, the AU requested the Internet Society to jointly develop the Personal Data Protection Guidelines for Africa (internetsociety.org).

Privacy International

Privacy International (PI) is a UK based charity that defends and promotes the right of privacy across the world.

Council of Europe

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data by the Council of Europe in 1981 is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data. (Council of Europe, coe.int)

Timeline of Events

Date	Description of the event
1950s	Creation of online computers
1974	United States Privacy Act
1981	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
1990	Privacy International Funded
	Creation of the “World Wide Web” (modern Internet)
1997	SixDegrees: first social media
1998	United States Children’s Online Privacy Protection Act (COPPA)

2004	Creation of Facebook
2014	Russian personal data localisation rules
	African Union Convention on Cybersecurity and Personal Data Protection
2016	EU General Data Protection Regulation
2018	Cambridge Analytica Facebook data harvesting
	UK Data Protection Act

Relevant UN treaties and events

- Guidelines for the Regulation of Computerized Personal Data Files, 15 December 1989 (A/RES/45/95)
- Human Rights and Scientific and Technological Developments, 20 February 1990 (E/CN. 4/1990/72)
- EU General Data Protection Regulation, 14 April 2016 (2016/679)
- United Kingdom Data Protection Act, 23 May 2018
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981

Previous Attempts to Solve the Issue

The United States attempted various solutions, tackling different aspects in data protection. For example, with the COPPA it focused more into protecting children's privacy through the parent's awareness of what the data was being used for. The issue with United States regulations is that, as previously explained, they do not apply to the country in general but to the State the regulation is from. Plus, there are no acts focusing on social media companies. According to Ieuan Jolly (2018), the Federal Trade Commission Act protects consumers and prohibits unfair or deceptive practices; the Financial Services Modernization Act regulates the collection, use and disclosure of financial information; the Health Insurance Portability and Accountability Act (HIPAA) regulates medical information; the HIPAA Omnibus Rule also revised the Security Breach Notification Rule requires covered entities to provide notice of a breach of protected health information; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act regulate the

interception of electronic communications and computer tampering, respectively. These acts and many more regulate types of data which are and may be handled by social media companies, being more comprehensive in the sense that they do not only apply to social media companies.

Overall, what countries and organisations try to achieve are regulations for companies to protect the private data of their users. However these are not exclusively social media companies despite social media being of the easiest ways to harvest users private data; still, legislation usually refers to them as included in data handling companies.

So is the case of the GDPR, which protects user data by setting a set of requirements companies that manage data need to comply with, and are checked to see if they do.

Data Protection Acts in all countries and organizations tend to include the aspect of data handling that social media companies have recently been criticized for. For example, after the Facebook scandal, the page changed its terms of service to make them clearer and reduce misinterpretations. As aforementioned, there is no data protection regulation which focuses on social media companies specifically.

Possible solutions

Personal responsibility of the users powered by the States is an option given the obstacles presenting an international legislation applicable to all countries may imply. Member States should focus in making sure individuals are aware and consent the use and handling of their personal data. This can be done through the media or even including short courses in schools.

Another option is to offer a base for each country to work a legislation on, which is what the EU did with the GDPR. This would express, for example, the need for every country to have a supervising organ on what each social media company does with its users' personal data. Otherwise, given the internationality of social media, a UN organ could be created so as to ensure this. It could express, also, the possibility of users to be able to

access what information is being stored on them and the uses that are being given to that information, and the right to claim it and delete it at request. Member States should also be expected to enforce a legislation complying with the base established by the UN after a reasonable amount of time.

Furthermore, countries should supervise social media companies' terms and conditions to make sure they are clear and comprehensible with no loopholes the company could take advantage of to get away with incorrect personal data handling. Plus, it would be good for users to be able to know who can access their personal data. Social media companies should also raise awareness among users about how to prevent their data from being accessed without their consent, through attractive or entertaining means such as animations and well structured text sections to increase the number of users they reach.

As Member States regulate the handling of personal data, the black market of personal data should be more limited as companies are supervised, making it harder to harvest personal data without facing legal consequences.

Regarding cybersecurity, it is quite challenging given that social media companies should have to limit the content allowed by censoring and banning; however, how far does this intervene with the rights of freedom of press and freedom of information?

Bibliography

Berzinya, Aigerim. (April 9, 2018). Data Privacy in Social Media: Who Takes Responsibility and Data Protection as a Priority Feature. Retrieved December 15, 2018 from https://turtler.io/news/data-privacy-in-social-media-who-takes-responsibility-and-data-protection-as-a-priority-feature

United Nations conference on Trade And Development. (nd). Data Protection And Privacy Legislation Worldwide. Retrieved December 15, 2018 from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Techquickie. (March 20, 2018). The History of Social Media. Retrieved December 18, 2018 from https://www.youtube.com/watch?v=cw0jRD7mn1k

European Commission. (2018). What is personal data?. Retrieved December 18, 2018 from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Kenton, Will. (January 25, 2018). Social Media. Retrieved December 18, 2018 from https://www.investopedia.com/terms/s/social-media.asp

Anonymous. (nd). Responsible conduct in data management - Data handling. Retrieved December 18, 2018 from https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/dhtopic.html

Privacy International. (nd). A Global Standard for Data Protection Law. Retrieved December 20, 2018 from https://privacyinternational.org/impact/global-standard-data-protection-law

Anonymous. (nd). EU General Data Protection Regulation (GDPR). Retrieved December 20, 2018 from https://eugdpr.org

CIO whitepapers review. (2018). What is Automated Processing. Retrieved January 11, 2019 from https://whatis.ciowhitepapersreview.com/definition/automated-processing/

Kukushkina, Mzhavanadze, Perevalov. (December, 2017). The Privacy, Cybersecurity and Data Protection Law Review – Edition 4: Russia. Retrieved January 11, 2019 from https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151296/russia

Anonymous. (nd). HG.org Legal Resources - The Law and Social Media. Retrieved January 11, 2019 from https://www.hg.org/legal-articles/the-law-and-social-media-31695

Federal Trade Commission. (March 20, 2015). Complying with COPPA: Frequently asked questions. Retrieved January 11, 2019 from https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

United Nations. (nd). Universal Declaration of Human Rights. Retrieved January 11, 2019 from http://www.un.org/en/universal-declaration-human-rights/

Chang, Alvin. (May 2, 2018). The Facebook and Cambridge Analytica Scandal, explained with a simple diagram. Retrieved January 11, 2019 from https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

BBC News. (April 4, 2018). Facebook scandal hit '87 million users'. Retrieved January 11, 2019 from https://www.bbc.com/news/technology-43649018

Merriam-Webster Dictionary. (nd). Of Privacy Legal Definition | Definition of Privacy by Merriam-Webster. Retrieved January 16, 2019 from https://www.merriam-webster.com/legal/right%20of%20privacy

Burgess, M. (2019). What is GDPR? The summary guide to GDPR compliance in the UK. Retrieved February 10, 2019 from https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

United Nations Conference on Trade and Development. (2016). Data protection regulations and international data flows: Implications for trade and development. Retrieved February 11, 2019 from https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

Kill, A. (2018). An overview of China's new cybersecurity law. Retrieved February 11, 2019 from http://www.mondaq.com/china/x/714616/Data+Protection+Privacy/An+Overview+of+Chinas+New+Cybersecurity+Law

United Nations Global Pulse. (2018). About | United Nations Global Pulse. Retrieved February 11, 2019 from https://www.unglobalpulse.org/about-new

Internet Society. (2018). Personal Data Protection Guidelines for Africa. Retrieved February 11, 2019 from https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/

Internet Society. (2018). Protecting Privacy and Personal Data Key to Digital Economy in Africa, says Internet Society. Retrieved February 11, 2019 from https://www.internetsociety.org/news/press-releases/2018/protecting-privacy-and-personal-data-key-to-digital-economy-in-africa-says-internet-society/

Appendix

I. EU GDPR document: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
II. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981 Convention) by the Council of Europe: https://rm.coe.int/1680078b37
III. United States of America 1974 Privacy Act: https://www.archives.gov/about/laws/privacy-act-1974.html
IV. Map showing countries with data protection and degree: https://www.cnil.fr/en/data-protection-around-the-world