



MUNESCO

Forum: GC5

Issue: The issue of data privacy with respect to the growing uses for big data.

Student Officer: Kayra Bahadır

Position: Deputy President

Introduction

Day by day, humanity gets more connected to exposing-exposing their feelings, their ideas, and themselves. Humans expose their values to others via many methods, which includes basic interactions such as speaking, hearing and touching. With years and years, a new and faster way of interaction appeared: the internet. Now, we are able to share ourselves to millions of people across the globe by a single click, and although seeming evolutionary, this technology comes with a cost.

As stated in the Princeton University Press, “The internet isn’t a chalkboard that you can write on and erase at your leisure. Once something is out there on the internet, it will more or less be there forever” (Anas, Web). This profound sentence has many to infer from it. It suggests that a post of yours can be reached by anybody after years, even if you deleted it. Furthermore, more than 71 percent of internet users are also users of global social media such as Instagram and Facebook. These websites can be considered as digital profiles of their users, meaning they obtain a lot of information regarding them. Aforementioned data can be used in ways users did not think they signed up for, but these companies indeed obtain the right to use the provided data, as usually stated in their *Terms and Conditions* agreements.

In the technology-led world of today, data is gold. Big companies are eager to process data which are called big data, and are able to manipulate their users in many ways such as making them buy products and etc.

In this chair report, we will analyze credible companies’ obtainment of big data and the consequences that came with it. It will be your mission to solve this issue with a solution which will be usable in this century of dynamic development, especially in the branch of digital technology.

Definition of Key Terms

Personal information (legally known as Personally Identifiable Information (PII) and Sensitive Personal Information (SPI): Personal information is regarded as any kind of information about an individual that identifies, locates and relates to them. As stated by the European Commission, personal data is “any information that relates to an identified or identifiable living individual”.



Data Breach: Data breach is the illegal exposure of obtained and collected personal or confidential data to an unauthorized party or environment.

European Union General Data Protection Regulation: The EU General Data Protection Regulation 2016/679 is a cyber-security regulation regarding the security of obtained data within the hands of major databases and cyber-companies. The regulation was primarily drafted in order to replace the present 1995 Data Protection Directive, which was not successful in tackling issues in the digital world of the 21st century.

Big data: The term “Big data” refers to obtaining extremely large amounts of data within the database. This data is collected for processing and analysing thoroughly in order to expose demographic and necessary information about the client of the market, in which the patterns, associations and further shapes of human behaviour and interest is displayed.

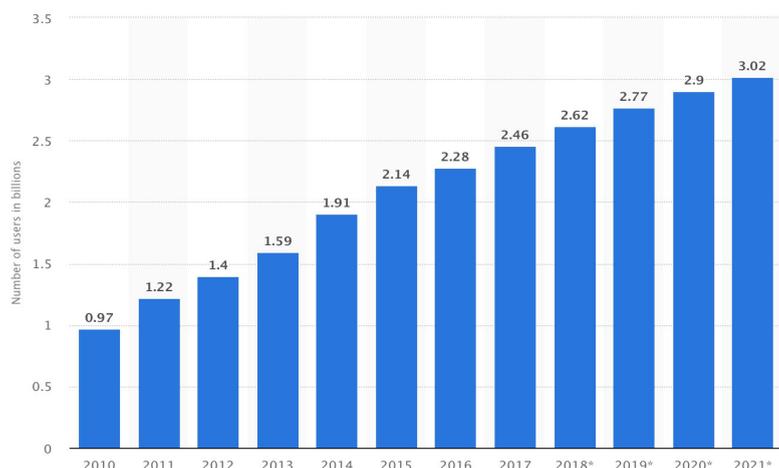
Background Information

The first digital database was invented by Edgar Frank Codd for American information technology company IBM in 1970. This database was a relational one, as it was used solely for relational purposes. The term database and its use changed a lot over time, as it turned from being an expensive establishment that government bodies obtained to easily created data pools obtained by any website with membership.

After public internet was exposed to citizens on August 6th, 1991, companies were created and websites were made. These websites started from single page informatory websites to membership requiring social-media platforms. After a year, in 1992, the European Union began proposing regulations upon this rising branch of communication while the United States of America stood with their Fourth Amendment, which was implemented a year after the invention of the digital database.

The security of newly adding up databases and the data they obtain started to become a concern after the 20th century. Companies like Facebook held up millions and billions of users, which came with new data to offer and enlarged the data pool of these social-service platforms. Below shows the increase in Facebook user count, projected until 2021.

Social-media companies had the honor of establishing their own big data, which made them





MUNESCO

targets to digital agencies such as Cambridge Analytica. Although the aforementioned numbers stress many people regarding assuring security for their data, Facebook was not that strict upon third-parties and their reach to data. Before the 2014 update, third-party apps had the right to further collect the data of users if their friends gave permission. Such lack of restrictions, combined with a large number of personal information, can be the cause of important scandals, especially in the digital world of the 21st century.

Timeline of Major Events

15 December 1971	The United States Senate obtained the Fourth Amendment, which prohibited unreasonable searches as a part of the Bill of Rights.
April 2010	Facebook created the platform Open Graph-an addition in which third-party companies obtained the right to ask for data from Facebook users, which directly gave access to data of the users' friends.
29 November 2011	The United States Federal Trade Commission (FTC) and Facebook came to a settlement which was named Consent Decree regarding data privacy of users.
2013	The app <i>thisisyourdigitallife</i> was created by Ex-Cambridge academic Aleksandr Kogan and his company Global Science Research. App's quiz spread around 270,000 Facebook users, who accepted to participate for "academic use only".
11 December 2015	The Guardian author Harry Davies exposed Cambridge Analytica's processing of millions of Facebook users' data for Republican Ted Cruz's presidential campaign.
17 March 2018	Carole Cadwalladr, alongside with an ex-Cambridge Analytica employee Christopher Wylie, counted on Donald Trump upon working with Cambridge Analytica to boost his campaign.
20 March 2018	The United States Federal Trade Commission (FTC) ruled out a new investigation regarding whether Facebook violated their 2011 agreement with the government agency on data privacy.
10 April 2018	Founder of Facebook, Mark Zuckerberg gave testimony to the U.S. Congress.
25 May 2018	The European Union General Data Protection Regulation 2016/679 was implemented across European nations, replacing the 1995 Data Protection Directive.



MUNESCO

Major Countries and Organizations Involved

The United States of America:

Being under spotlight regarding the situation and previous incidents related to the situation, US obtains both the sources of the incidents and many steps taken to prevent them. After the Facebook scandal, U.S. government started evaluating European Union's General Data Protection Regulation and possibly implementing it or other regulation based on EUGDPR. The United States Federal Trade Commission has taken steps regarding social enterprises and maintaining supervision over huge databases like Facebook, such as the Consent Decree in 2011.

The European Union:

The European Union has not been affected by such similar data breaches but yet been very prepared for them. They have implemented the Data Protection Directive in 1995 and refreshed it in 2018 by the General Data Protection Regulation. The United Kingdom (currently a legal member of EU) has fined Facebook 500,000£ while the European Parliament's Civil Liberties Committee called for a full audit of Facebook.

The African Union:

The African Union, alongside with the Economic Community of West African States (ECOWAS), have shown their effort in this issue by many ways. They have designed and hosted the African Union Convention on Cyber-security and Personal Data Protection, which was a significantly influential step to take. They have shown many times that they are keen on collaborating with other nations and foundations, when they jointly organized a workshop regarding cybersecurity and related agenda items with the Council of Europe.

Previous Attempts to Solve the Issue

One of the first attempts upon this issue was the addition of the *Fourth Amendment* to the Constitution on December 15, 1971. Although tackling the issue of personal privacy by many means such as but not limited to unreasonable searches and questioning, this amendment did not really consider the upcoming technology and today's internet. In 1995, the European Parliament accepted *Directive 95/46/EC* (also known as *Data Protection Directive*).



MUNESCO

This newly created directive had a clearer perspective on the technology and also considered digital data. In 2011, the United States Federal Trade Commission (FTC) and Facebook came to a settlement called *Consent Decree*, which handled loopholes in Facebook's functioning and created guidelines Facebook had to follow while functioning for the well-being of personal data they obtain. This was not enough, as Facebook came into a verdict that they violated this settlement, which costed 87 million user's personal data being exposed to Cambridge Analytica. In 2014, Facebook revisited and edited rights third-party apps obtained and limited their reach to permitter's data. Since then, no significant data breach was observed.

Although playing a major aspect whether from its governing choices or being homeland to big data owning companies, the world besides the US has also taken a lot of action regarding the issue. For many years, tens of conventions and legislations were established. In 27 June 2014, the African Union (AU) hosted African Union Convention on Cyber-security and Personal Data Protection, which targeted the issue with the collaboration of African states. In addition to the AU, the Economic Community of West African States (ECOWAS), had also taken a lot of steps in this path, most significantly with their 2010 Supplementary Act on Personal Data Protection. Furthermore, the Asia-Pacific Economic Cooperation (APEC) nations established the APEC Data Privacy Framework for the security of data in the region's countries. Singapore was the last one to sign the legislation, date being 7 March 2018.

Possible Solutions

A possible solution would be to inform the public regarding the issue, so they can be more informed when they use these public platforms. This can be established by government reach, i.e. in digital platforms. However, governments acts would be satisfactional without the collaboration and support from social media companies. The public shall establish the trust to these companies via the transparency of social media platforms regarding the issue.

Furthermore, other countries might be urged to count the EU's present General Data Protection Regulation as a blueprint for them to create their own legislation upon the issue. This would enable for them to base their own legislation to a already-approved and respected one, as the present EU legislation has shown nothing but success. This can also be done in a conference, where government officials and UN body representatives would be present to share their thoughts regarding the issue and possible additions to international and national laws. A suggestion would be to include representatives from grand database owner companies like Facebook, as the world has already seen examples of how governments bargained and forced companies to follow specific limitations if they wanted to continue their presence in their nation.



MUNESCO

Additionally, a new establishment under UNCTAD Division on Technology and Logistics can be created, which can help countries with low technological capabilities and experience to create suitable legislations and laws to be added in their law. Although obtaining a legislation, some of these laws include major gaps and loopholes within them-i.e. the exclusion of small businesses in the case of Australia & Canada. The improvement already existing establishments are incredibly needed for such nations. This establishment could be a sub-branch specific for this context, as no such elaborate platform is present today.

Useful Links For Further Research

<https://www.privacyinternational.org/>-This organization is an advocate for ones who have been harmed by the data movement as a result of weak legislations regarding the matter. The website provides useful information regarding the issue.

https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

This official page of UNCTAD regards the Data Protection and Privacy Legislation Worldwide, which is one of the most significant steps UN has taken in this matter. Additionally, this website has an interactive world map in which shows which nations established a legislation on this issue.

https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

This official publication includes many approved information regarding the issue while categorizing it for easy reach.

<https://ccdcoe.org/ecowas.html>

This website regards the steps ECOWAS has taken regarding the issue in hand. This website is significantly helpful for African nations to get to know their policies and their previous steps upon this matter.

Bibliography

Anas, Angelica. *Posting Remorse: Deleting Isn't Permanent on the Internet*. Princeton University Press, 2013.

“Personally Identifiable Information.” *Wikipedia*, Wikimedia Foundation, Inc.



MUNESCO

“What Is Personal Data?” *Together Against Trafficking in Human Beings*, The European Commission, 1 Aug. 2018,

“Facebook Users Worldwide 2018.” *Statista*, Statista, www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Associated Press. “UK Fines Facebook Over Data Privacy Scandal, EU Seeks Audit.”

Lomas, Natasha. “Europe's Parliament Calls for Full Audit of Facebook in Wake of Breach Scandal.”

Bloomberg. “Facebook May Have Breached a 2011 Consent Agreement, FTC Says.” *Fortune*, Fortune, 29 Mar. 2018,

“Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises.” *Federal Trade Commission*, 30 Dec. 2013,

“Facebook–Cambridge Analytica Data Scandal.” *Wikipedia*, Wikimedia Foundation, Inc.,

Davies, Harry. “Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users.” *The Guardian*, Guardian News and Media, 11 Dec. 2015,

Rosenberg, Matthew, et al. “How Trump Consultants Exploited the Facebook Data of Millions.” *The New York Times*, The New York Times, 17 Mar. 2018,

Meredith, Sam. “Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal.” *CNBC*, 10 Apr. 2018,

“Relational Database Management System.” *Wikipedia*, Wikimedia Foundation, 29 Jan. 2019,

“Edgar F. Codd.” *Wikipedia*, Wikimedia Foundation, 10 Dec. 2018,

<https://www.adweek.com/digital/a-researchers-quiz-app-deceptively-harvested-data-for-political-research-facebook-alleges/>



MUNESCO