ZYGMUN

JR.MUN COMMITTEE

PROTECTING THE RIGHT OF PRIVACY IN THE DIGITAL AGE

XINYING SUI
SZYMON KAPUSTKA

Table of Contents

I. Introduction

The internet has shown a great amount of possibilities to access and exchange information, especially in the digital era, where there have been a significant increase in use of technology, and the effect of it's many possibilities, such as social media platforms. Upgrades and advances have been structured to explore and create more developed and sophisticated technology. The resolution on the right of privacy in the digital age, adopted on 18 December 2013 was the first step towards the right of privacy and network security, established by the UN. Restating the human rights measure that needs to apply to the interception of communication and collection of personal data. The amount of individuals using digital media is rapidly increasing. 91% of internet users access email, showing that the majority of internet usage is performed by sending and receiving digital messages. Proving that the internet is commonly used in relation to personal information and data as shown by communication purposes. Therefore, individual's privacy is extremely vulnerable in the digital age, as personal data on Google, Facebook and Microsoft can possibly become exposed.

In 2018, one of the biggest controversy regarding this issue occurred. The scandal affected millions of Facebook users, as Cambridge Analytica (US and UK), a data-marketing firm controlled by the organization SCL Elections Ltd., managed to capture non-authorized personal information from approximately 87 million US Facebook profiles. The data was acquired for political advertising and building voter profile. Personal space is so minimal that it's almost nonexistent, affected by the many privacy issues that are often caused by bias and improper actions.

II. Definition of Key Terms

Digital Age
The era started in the 1980s and is still ongoing. Otherwise also referred to as the informational age, it's a historical period were many actions and knowledge are done by the computer and newly advanced technology. A great amount of information is available due to the computer, and it's many abilities, which allows us to store and transfer necessary data.

Subpoena
It is a legal command that orders an individual to give a testimony on a specific subject, in front of the court or other proceedings as a witness. This written regulation can be challenged, only by informing the court, as if in failure to comply such an order it may lead to a punishment**.**

Personal Data
It's a set of information that belongs to an individual. This information is related to both identified and identifiable person, meaning that the data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name. These also include all data which are or can be assigned to a person in any kind of way, such as personnel number of an individual.

Cookies
A web cookie is a piece of data that contains data about online users. It is sent from a webpage and put away into the user's internet browser and utilized on the page without their consent. Like the username and password that allows you to enter the computer and use its network.

Surveillance
Alludes to the close and nonstop perception or watch over a place, individual, or community. The watch is commonly over somebody who is a suspect or a criminal. This can also relate as an action don online, as computer activity and data stored on a hard drive, or data being transferred over computer networks such as the Internet can be monitored.

III. General Overview

a) Internet Censorship

It's common in the digital age and internet censorship usually puts restrictions on what information can be publicized or viewed. National Governments take a big role in controlling what can be seen online, most countries have moderate Internet censorship, however some are more severe than others. Internet censorship is used to ban access to information that is copyrighted, harmful, sensitive or other illegal digital content that can be found on websites, social media services or file sharing services. All countries have censorship laws. However, Iceland is known as a country with the least limited freedom online, meaning that their online laws aren't that strict. According to Statista, Iceland is ranked first as the country with the least censored internet, followed by Estonia and Canada. Internet censorship does not only, set a limit on content but can cause violations of users rights and freedom of speech. Censors seek to limit freedom of thought and expression by restricting visual arts, music, words, symbolic messages and freedom of association. Placing restrictions on internet users should be well moderated by the government not depending on culture, religion or most commonly political reasons.

b) Computer and Network Surveillance

One of the many factors affecting privacy and secure use of internet is computer and network surveillance, that captures your stored data while monitoring your activity online. It often involves data stored on a hard drive or information that is being transferred through networks. The monitoring commonly refers to, and is done by the government, criminal organizations or individuals. The National Security Agency (NSA) and other agencies can have possible access to your digital devices through built in back doors. In other words this means that, they can read your messages, go through your calls, capture pictures and videos of you or steal your files whenever they need to.

In 2013, former Central Intelligence Agency employee and subcontractor, Edward Snowden also known as the American whistleblower, revealed that the US and the UK security services are routinely collecting, processing and storing vast quantities of global digital communications. Tempora is a mass-surveillance system allegedly run by the Government Communications Headquarters (GCHQ), which the UK didn't deny nor confirm its existence. Mass surveillance on a particularly industrial level is unlawful, clearing aside our entitlement to protection and the freedom of speech and expression. It changed the perspectives of many societies and member states around the world, of to what extinct your rights to online privacy can be violated.

c) Your Rights of Personal Information

The internet is a huge network where everything you posted, wrote or created can be found. A lot of the personal information that you posted on the internet is exploited or made use of without your consent. The privacy that is required for every individual is drastically minimizing in the Digital Age, and cases with theft of data aren't decreasing. Having your identity stolen can compromise your life on the daily bases, as well affect activities and sabotage your reputation, both privately and professionally. The modern technology has the ability to transfer information freely and quickly, therefore its necessary to know online boundaries to protect individuals from many aspects of social media platforms and companies. One of the most recent data breaches was the breach of Equifax, an American multinational consumer credit reporting agency, that announced a data breach which exposed sensitive and important personal information of 147 million people, back in 2017. Equifax disclosed that a failure to patch one of its Internet servers against a pervasive software flawed a component of the web. Equifax agreed on a $700 million settlement due to this tremendous data breach.

IV. Major Parties Involved and their Views

a) United States of America (U.S.A)

It is a very common status of modern society that about six-in-ten U.S. adults state they do not think it is possible to go through daily life without having data collected about them by companies or the government. The developed technology and possibilities of the internet often contribute to their thinking. Additionally, the United States of America are a country where nearly all social media apps and many technical advances were founded. Therefore, they hold a major importance in this issue, as despite their contribution to protecting personal privacy, many important circumstances regarding this problem occurred. One of the most recent issues was when the US congress called the CEO of Facebook, Mark Zuckerberg for a testimony following his company's scandal with Cambridge Analytica. However, there are many laws referring to internet use and personal data in the US. The most remarkable ones include: Electronic Communications Privacy Act (ECPA) and The Consumer Online Privacy Rights Act (COPRA).

b) European Union

The EU has been aware and concerned of the privacy issues, that are increasing rapidly in the Digital age. The General Data Protection Regulation (GDPR) is a law protecting data and privacy in the European Union. The role of GDPR is to manage the protection of data that belongs to the EU citizens. The process relating to protection of individuals with concern to the managing of personal data by EU institutions established a European Data Protection Supervisor (EDPS). Which is an independent UN body responsible for checking the use of information of security data rules inside European Institutions and for looking into complaints. The regulations are an essential part of ensuring a well secured privacy for the citizens of EU. All member states belonging to the European Union are under the concern and necessity to have their companies and partner comply with the unions regulations, without any exceptions.

c) People's Republic of China

Having many laws and regulation when it comes to the internet, China has a great amount of policies and is the major party in the internet censorship globally. China allows their citizens to see their high security and control. The have regulations that relate to personal information and use of internet. In 2002 The Internet Society of China, a non-governmental organization (NGO) that incorporates individuals from the whole Internet business including scientists, researchers and students, established the Public Pledge of Self Discipline in order to set an agreement between their own internet industry and corporation that develop and operate sites in China. This arrangement was to prevent transmission of information associating with breaking laws or suspicious threats. Additionally, many common social media sites and platforms like Facebook,

YouTube or Instagram are banned, but that doesn't mean that there aren't any online privacy laws and matters. The application Zao, used by many in China, not long ago the public found out that it was allowed to use their created images and/or videos for free. Which created outrage, so the company stated that they will not be taking the users' content for free without their consent. The public by years is starting to notice more of their legal rights online and 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.

d) Russia

Fundamental means of data protection law can be detected in the Russian Constitution. Being one of the many members that established the Strasbourg Convention for the Protection of Individuals with esteem to Automatic Processing of Personal Data , that was ratified by Russia in 2006. It allows individuals to have a more secure and private online data without any unlawful or accidental access, taking account of the increasing flow across frontiers of personal data undergoing automatic processing. Additionally, the deep packet inspection (DPI) is an advanced method of examining and managing network traffic. The Government of Russia has been getting a great amount of critics recently after excessive blocking of internet access and for using internet regulations for censorship. Indeed, even without DPI innovation completely working in Russia, at any rate 85,246 sites have just been blocked as of June 10, 2021. In this specific situation, multiple local and worldwide Human Rights associations communicated worries over the obscure and extrajudicial impeding of sites encouraged by DPI technology.

V. Relevant United Nations Documents

Personal data Protection and Privacy Principles - The General Data Protection Regulation (GDPR) sets out seven principles for the lawful processing of personal data and information. They consist off the following; Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security) and Accountability. These principles outline the importance of privacy which is an important factor of Human Rights. They state the required and appropriate regulations that apply to every individual.

Digital Identity Management & Electronic Authentication - This report/document 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. Digital identity has four main parts; credentials, user information, character information, and reputation.

VI. Questions to Consider

- Should member states use network surveillance and collection of data to monitor terrorism, cyberterrorism and acts of violence?
- How can society influence the rapid changes and developments in technology and computer network?
- How does internet censorship violate Human Rights when controlled by the government?
- Is EDPS a necessary establishment to ensure that European bodies respect the right to privacy when developing new policies? Should a principal data protection legislation be established in every country?
- Do major advance in technology herald fundamental social and economic change when undertaken by organizations?
- How do institutions impact privacy rights in the modern days? What needs to be considered in those institutions?
- Is it legal for information gathered by cookies on social media sites to be used beyond advertising?

VII. Conclusion

Having you information and data on the internet is often a necessary aspect of your daily life. A great amount of individuals works online, specifically about 3.5 billion of people around the world have an internet based job. Your information can become extremely vulnerable in the Digital age, therefore its necessary to establish or reinforce regulations and laws, as well as create organizations that support this matter.

Undertaking the legislation aspect is the primary obvious effectuation from preventing these problems in happening further in the future. Implementing effective laws against such issues will not only raise awareness of the issue but also hopefully decrease the number of criminals and cybercrime in general. It is moreover critical to keep such legislative bodies with the latest with updates that cover future and arising innovations. Seeing how rapidly technology and innovations change in the Digital age, the key for individual privacy is keeping regulations, laws, and treaties updated frequently. Strengthening network security should be taken into consideration and developed into an organization with a purpose of monitoring social media sites

to detect any unlawful act or doing that would violate users privacy. This organization would have the legal right to investigate any concerns and demand reports from social media platforms to see if there are any issues relating to this question at hand.

The increasing amount of violations against privacy and the concerning amount of data breaches relating to corporations as well as personal substances, proves the importance of addressing this topic by the states before it becomes irreversible due to the expanding digital technology

VIII. Bibliography

"A Brief History of US Federal Data Privacy Laws." *Tiki-Toki*, www.tiki-toki.com/timeline/entry/480661/A-Brief-History-of-US-Federal-Data-Privacy-Laws/. Accessed 10 Jan. 2021.

"Data Protection and Online Privacy." *Your Europe - Citizens*, europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-onlineprivacy/index_en.htm. Accessed 10 Jan. 2021.

Lockwood, Bret. "10 Technology Challenges." *SGR Law*, www.sgrlaw.com/ttl-articles/10-technology-challenges/. Accessed 10 Jan. 2021.

"Mass Surveillance." *Amnesty International UK*, 18 May 2020, www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden. Accessed 10 Jan. 2021.

Nolasco, Denis, and Peter Micek. "Defending the right to privacy globally: 8 key recommendations for the digital age." *Access Now*, 25 Apr. 2018, www.accessnow.org/ defending-the-right-to-privacy-globally-8-key-recommendations-for-the-digital-age

/. Accessed 10 Jan. 2021.

Petronzio, Matt. "The Countries with the Most and Least Internet Freedom." *Mashable*, 17 Dec. 2014, mashable.com/2014/12/17/internet-freedom-countries/?europe=true#I__rGrhXWmqw. Accessed 10 Jan. 2021.

"Protection of Personal Data." *European Commission*, ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en. Accessed 10 Jan. 2021.

"U.S. Charges 4 Chinese Military Officers in 2017 Equifax Hack UK." *Krebs on Security*, 10 Feb. 2020, krebsonsecurity.com/tag/equifax-breach/. Accessed 10 Jan. 2021.

"What is Internet Censorship?" *Iplocation*, 18 July 2016, www.iplocation.net/internet-censorship. Accessed 10 Jan. 2021.

Xie, Echo. "Latest crackdown on Chinese social media sees dozens of high-profile Weibo accounts silenced." *South China Morning Post*, 9 Apr. 2019, www.scmp.com/news/china/politics/article/3005281/latest-crackdown-chinese-social-media-sees-dozens-high-profile. Accessed 10 Jan. 2021.