HISAR SCHOOL

JUNIOR MODEL UNITED NATIONS 2018

“Globalization: Creating a Common Language”

Economic and Social Council

Preventing the marketing of personally identifiable information

HISAR SCHOOL JUNIOR MUN

RESEARCH REPORT

Recommended by: THIMUN

Selin Gören

Forum: Economic and Social Council

Issue: Preventing the marketing of personally identifiable information

Student Officer: Selin Gören (Vice President)

Introduction

As the world becomes more and more globalized every day, people start to develop better ways to connect with each other regardless of their location. This fast developing technology, without any doubt, serves to create a common language in a highly globalized world. However, globalization also has its own disadvantages and developing technology raises concerns regarding privacy, personal data protection and freedom/autonomy of companies/websites.

It's therefore crucial for United Nations to take action and prevent the marketing of sensitive information which the individuals share. Even if they don't trust the companies, people feel obligated to share their information simply because some companies don't offer the user any other chance. In a highly globalized world, it's nearly impossible for a person to abstain from using any and all internet services. Therefore this problem affects every individual living in our current era, whether that person is a CEO or a teenager.

This research report is prepared for the delegates who're willing to solve this major issue surrounding our highly globalized world which threatens the efficiency/justifiability of technology.

Definition of Key Terms

Personally Identifiable Information(PII): The data which can be stored and then later used to locate, investigate or contact an individual which is unique to every person.

Direct Identifiers: Information that can lead to the identification of the person directly such as the person's ID Number

Quasi-identifiers: Information that can lead to the identification of the person only when combined with other quasi-identifiers such as age, gender, race, name.

Big Data: Pieces of really detailed data that are being collected by the companies, which are arriving from multiple sources and in multiple formats.

Cyberattack: An attempt to damage or steal information from a system or network by hackers.

General Overview

As the United Nations Conference on Trade and Development (UNCTAD) puts it, "Creating trust online is a fundamental challenge" in our globalized world. Although the data individuals provide fuel much of the commercial activity in the websites the usage of this data can put the privacy of people at stake, therefore can damage the core values UN upholds regarding data protection in the digital age.

One of the underlying problems beneath the issue at hand is the lack of uniformity between the legislations of different countries. Some of them have concrete measures against the marketing of PIIs whereas some others are yet to take action. This affects international businesses and trade greatly, since every country has different approaches towards data privacy.

Surely, with the easy access granted to all users via the internet and cell phones, there is a fast-growing supply of all kinds of data. This reservoir of information which is part of the Big Data is processed, interpreted and sometimes even sold by the companies. While this huge net of data enables the companies to find better ways of communicating with their customers and to draw better conclusions it can also get extremely dangerous for the customers, if not protected by the companies. This is currently raising many questions regarding the reliability of the companies when it comes to protecting the privacy of the customers. The variety and the importance of "Big Data" also entices cyber terrorists to attack the databases of some websites to steal information. Indeed, not all the companies are sensitive towards these kind of data and the number of scandals regarding the marketing of personally identifiable information increase day by day. Among these scandals Facebook's misusage and selling of personal information is one of the most recent and alarming ones. Facebook has admitted that it's been selling access to personal information to other companies which show specific ads targeting your interests. This fact shows that even the biggest digital companies may violate the privacy rights of customers today therefore specific measures should be taken to tackle the issue. Even though technically the users are asked to sing a customer agreement while signing up for such internet services, the information that they provide may be used for the affairs that the customers don't agree at the first place. To sum up, companies take advantage of the customers' trust to reap profit through commercial activities.

Major Parties Involved and Their Views

European Union: EU firmly believes that strict data protection policies must be developed and implemented in all countries to establish trust between the client and the company.

USA: In the US there isn't any single law regulating the distribution of PII, and the existing ones aren't as elaborated as the ones EU is proposing. The US generally establishes self-regulatory frameworks however a standardized law at federal levels is yet to come.

People's Republic of China: In China, just like in US, there are separate legislations regarding the protection of personal data instead of a comprehensive law. In June 2017, Standing Committee of the National People's Congress adopted "The PRC Cybersecurity Law", which was the first step taken on the national level to regulate data protection. In addition, China's current criminal law prohibits the sale or illegal access to the citizens' personal information.

Russian Federation: Russian Constitution includes specific articles regarding the data protection. The constitution establishes the data privacy of each individual in articles 23 and 24. On July 22 2014, these articles were amended so now any website/organization which violates the terms is blocked by the state

Timeline of Events

Date of Event	*Description of Event*
1970	*The first data protection laws were implemented as the computer became a part of the daily life.*
14 December, 1990	*The UN General Assembly passed the resolution 45/95 which focused on regulation of computerized personal files*
24 October 1995	*Directive 95/46/EC was adopted regarding the free movement of personal data is adopted.*
2015	*United Nations appointed a Special Rapporteur to report the changes in the international data privacy*
2015	*Relevant policy responses were adopted to the Sustainable Development Goals to protect the information and communication technologies (ICTs)*
24 May 2016	*EU adopted the General Data Protection Regulation (GDPR)*
23 March 2017	*The Human Rights Council adopted resolution 34/7 on "The right to privacy in the digital age"*
November, 2017	*Guidance Note on Big Data was published by United Nations Development Group*
March 21, 2018	*Facebook misuse of personal information scandal leaked*

Treaties and Events

- In 1948 Universal Declaration of Human Rights was issued by UN, which touched upon the right of privacy in Article 12.

- The International Covenant on Civil and Political Rights in 1966 was signed by 160 countries. Article 17 talked about data privacy.
- In 1981, the first legal binding international treaty on data protection was issued by the Council of Europe, namely Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data. An additional protocol to the convention was issued in 2001 to enable the authorities to monitor the national data protection.

Evaluation of Previous Attempts to Resolve the Issue

Starting from 2016, developing countries have been increasing their attempts to adopt internationally applicable data protection policies but most of these attempts failed due to three main reasons: The countries couldn't find the necessary funds, an applicable time and the required knowledge to implement the laws. Therefore, in many countries, such measures were failed to be taken.

Also, businesses were concerned about UN's actions to implement international data protection laws because they thought that too strict regulations would scare the customers and stakeholders. They believed that such regulations would reduce the commercial activities and prevent the commercial agencies from reaching the complete data base. Believing that this would hurt their profits, some of them opposed to these new changes and therefore made it harder for the countries to implement those laws since they needed the cooperation of private sector that is currently contributing to Big Data.

Possible Solutions

As mentioned in the overview section, creating a common language between countries when it comes to the legislations regarding the protection of private data and the punishment for marketing of PIIs is key to solve the issue at hand. Therefore, one of the main objectives of UNCTAD must be to reduce the gap between the privacy policies of different countries. If every country has a concrete punishment against the cybercrimes and the marketing of personal data, then an agreement can be reached. As UNCTAD mentions "internationally compatible data protection regimes" must to create trust and predictability for the stakeholders and customers.

These laws must center around seven main points according to the UNCTAD report: Addressing gaps in coverage, addressing new technologies, managing cross-border data transfers, balancing surveillance and data protection, strengthening enforcement, determining jurisdiction and managing the compliance burden. If all countries take action on these seven areas and include them in their regulations, the marketing of PIIs can be prevented internationally. Also the user agreements must become more clear and transparent so that the users will not be tricked into providing their information. Last but not least, the customers' awareness of the issue should be raised through campaigns if PIIs are to be prevented.

Bibliography:

DATA PRIVACY, ETHICS AND PROTECTION GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA." *United Nations Development Group*, undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf.

"Data Protection Regulations and International Data Flows: Implications for Trade and Development." *UNCTAD*, Data protection regulations and international data flows: Implications for trade and development.

"Data Protection Laws of the World." DLA PIPER, 2017. Accessed September 22, 2018.

"International and Foreign Cyberspace Law Research Guide: Introduction." *Guides*, guides.ll.georgetown.edu/c.php?g=363530.

"OHCHR | Call for Inputs to a Report on the Right to Privacy in the Digital Age." *OHCHR | Convention on the Rights of the Child*, www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportPrivacy.aspx.

Picchi, Aimee. "Facebook: Your Personal Info for Sale." *CBS News*, CBS Interactive, 21 Mar. 2018, www.cbsnews.com/news/facebook-your-personal-info-for-sale/.

"Practical Law." *Practical Law UK Signon*, uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default.

"Protecting Personal Information: A Guide for Business." *Federal Trade Commission*, 6 Sept. 2017, www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

"Sharper Insight. Smarter Investing." *Investopedia*, Investopedia, www.investopedia.com/.

"The History of the General Data Protection Regulation." *European Data Protection Supervisor*, 12 Aug. 2016, edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.