Forum: Youth Assembly

Issue: Ensuring the protection of personal data

Student Officer: Deniz Oray

Position: Co-Head

INTRODUCTION

As we have moved into the 21st century, the usage of the Internet has been increased from 16 million users in December 1995 to 4.383 million users in March 2019, which corresponds to an increase from 0.4% of the population to 56.8%.[1] With this huge increase, there have been scandals, such as the Cambridge Analytical and the Facebook scandal in 2018, as well as the Equifax Credit Disaster in 2017. Personal data is known as the information revealing a person's identity including their gender, phone number, home address, and name. Especially since the increasing number of identity fraudsters and data breaches, as well as the disobedience against the safety and privacy regulations, ensuring the protection of personal data has been a major concern for many nations. [2]

1- An image regarding personal data protection and safety

Personal data should be taken care of for a designated, straightforward and constitutional purpose while collected in order to warrant an accordant manner of processing for the same reason. The aforesaid management of personal data

[1] "Internet Growth Statistics 1995 to 2019 —the Global Village Online." *Internet World Stats*, www.internetworldstats.com/emarketing.htm.

[2] (https://www.acc.com/docket/articles/ensure-safe-personal-data-protection-handling.cfm)-.

should be necessary, pertinent and limited to the specific reason, for which are processed.

Any type of loss, unsanctioned access, qualification, use, or revelation of the data belonging to a citizen may be deemed as identity theft. It is therefore vital to take measures to ensure both the protection and privacy of the data and the systems, which include the data.

Establishing and meeting the highest possible data protection standards are crucial for ensuring the safety of personal data. Until today, there has been an international set of regulations on the Protection of Personal Data, a report of the United Nations High Commissioner for Human Rights, the General Data Protection Regulation by the European Union, the Data Protection Law Enforcement Directive, and the Personal Data Protection Commission, in order to tackle threats, such as data breach or identity theft as a result of unsuccessful data protection.

DEFINITION OF KEY-TERMS

Personal Data:

Personal data is the information regarding a specific person, which permits or may permit the identification of this person. This may include his name, address, social security number, identification card number, or email.

Sensitive Data:

Sensitive data is the information, which is safeguarded from unjustified divulgence. As stated by the EU, the following personal data is considered as ‘sensitive’ and should be dependent on particular processing conditions, some of which are personal data divulging racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; genetic data, biometric data organized simply to identify a human being; health-related data; and finally, data regarding the sex life or sexual orientation of an individual.

Big Data:

Huge data sets that can be perused in regard to computers to show patterns, trends, alliances concerning human behavior and interlinkages.

Data Protection:

The protection of a person's identifiable information and data, including photographs, names, birth date, etc.

Identity Theft:

Identity theft is the type of fraud, which occurs when imposters steal an individual's personal information revealing your identity such as your name, your ID, phone numbers, and financial information in order to make transactions or purchases.

Ransomware:

Aiming to attack businesses, ransomware is defined as a type of malware, by which the malefactors gain access to the company or individual's information. Furthermore, the indispensable data (files, systems) is locked up. To regain access to the data, the company is obliged to pay a fee in the form of Bitcoin or other cryptocurrencies.

Malware:

Malware is any type of software created to damage computer files and systems. By faking a warning message in regard to a virus, Malware steals sensitive data from the users letting them into a virus type of websites.

Phishing:

This type of breaching takes place when a trustworthy and respected institution is mimicked for the purpose of stealing personal information and sensitive data. This type of data usually contains very personal facts. Phishing may occur as a pop-up on the browser, an email containing a link, or a person on a phone call faking to be the representative of the company.

Denial of Service (DoS)

The DoS breach, also known as the Distributed DoS, on a large-scale disables access to webpages and websites. As a result of these attacks, a majority of the online sites in specific areas may be deranged. Privacy Rights Clearinghouse, which gives outlines on the impact of data breaches on consumers, stated that the information accommodated includes data useful to fraudsters, such as Social Security numbers.

Data Brokers:

Data brokers are organizations, which gather information on a consumer and then sell the data to fellow data brokers, citizens, or other businesses.

BACKGROUND INFORMATION

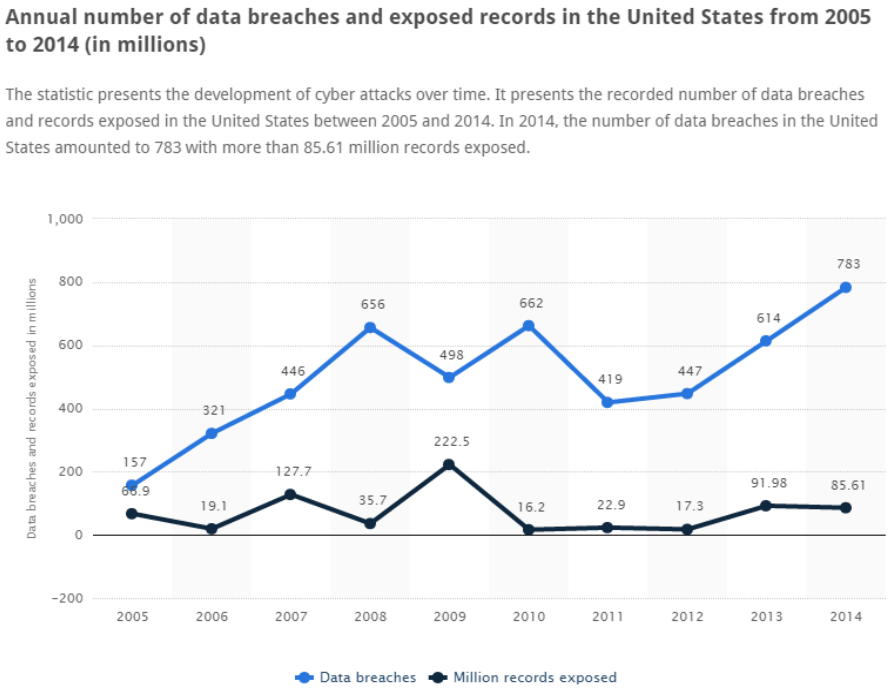
[3]

2-The GDPR

[3] "GDPR." *DecisionWise*, decision-wise.com/gdpr/).

Data Breaching:

As the technology has developed, there have been several data breaches over the years. A data breach is an occurrence, which results in the theft, the view, or an unwarranted use by an individual of protected, perceptive or classified data. Payment card information (PCI), personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property are all part of data breaches. Breaching a company's data has become undemanding with regard to the convenience of ingress to restricted networks as a result of sensitive data maintained on local business machines, on firm company databases, or cloud servers.



Data breaching has existed since companies and individuals have maintained records and stowed private information. Before the computer age, an unauthorized view of a patient's medical file would be considered as a data breach. However, in the 1980's, the number of data breaches increased. Later on, in the 90's and early 2000's, the individuals became more aware of the potential threat of data breaching. The HIPAA (Health Information Portability and Accountability Act) regulation, laws, or the PCI (Payment Card Industry) Data Security Standard have been established to furnish organizations and companies contending with specific types of sensitive consumer information with relative instructions. These enactments constitute on the one hand, a structure for the needed safeguards and on the other, storage and provide information on how to handle sensitive data. However, these rules are not present in every industry and cannot completely tackle the issue of data breaching.

3- A graph on data breaching in the US.

In 2019, data breaches may often affect millions of people and individual records. With the improvement of technology and growth of electronic data, data breaches have been a major upset for both consumers and enterprises. [4]

Identity Theft:

Identity theft may also occur as a result of publicly exposing personal data via breaching or other ways. Identity theft, as previously mentioned, is a crime related to the insecure communication in many countries, giving accessible information to websites (secure or insecure) and shops, as well as the immoderate use of electronic devices due to the Internet. The thieves may also use someone's information on their gain to exit a country illegally, to sell drugs and bring other substances in to the country, along with increasing the cybercrimes and laundering money. Identity theft has been happening all around the world in high rates. In 2017, countries, like the United Kingdom (UK), developed initiatives, such as the Banking Protocol, as a solution to the increasing identity fraud. This facilitated the protection of customers, since it is a ground-breaking response scheme, through which branch members can call the Trading Standards and the police to track down suspected frauds happening. In 2017, while the Protocol was available to the police forces, £13.3 million of fraud/theft were precluded and 129 arrests were made.

Data Brokers:

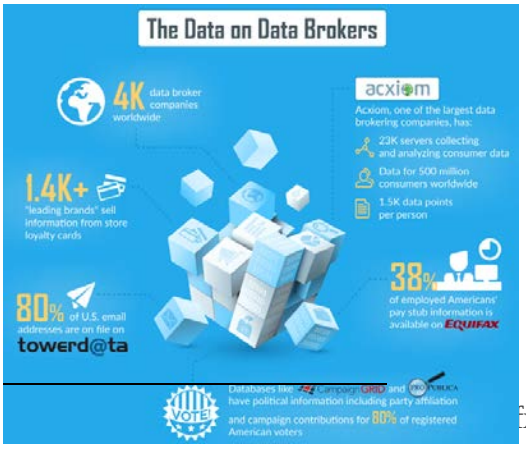
The process of tracking the data brokers is really challenging since the brokers don't have a close relationship with the individual they are stealing the data from. Therefore, the victims usually have no clue on what happened on their data. Data brokers are divided into three categories. In

[4] "U.S. Data Breaches and Exposed Records 2018: Statistic." *Statista*, www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

some search sites, by a simple name or phone number, the personal data of the users may be accessed. They may get this information either by paying an amount of money or not. Some of these search sites are PeopleSmart or Peek You. These are usually used to write a postcard to a friend, but may be used by brokers when they receive court records or other personal information, such as addresses. A few data brokers, like Datalogix or Equifax, focus on marketing by classifying individuals according to their age, the number of children they have, and their ethnicity. These sites may result in high-risk classifications, such as pushing the viewer to engage in risky behavior. Unfortunately, there is not any process in removing or changing the information posted. ID Analytics falls within the last category of data brokers as they provide risk alleviation materials to reveal identities and contribute to perceiving fraud. Unless the information is imprecise, this type of data brokers is the least exasperating for consumers.

Paul Stephens, the Director of Policy and Advocacy at Privacy Rights Clearinghouse has stated that “If you can get information on someone online, you might be able to impersonate them or use their credit history, or perhaps get into a password protected website if you can answer security questions about people.” “It certainly can be used by stalkers to find out the address of someone; it can be used by someone who wants to harass you by phone if they’re able to get your phone number.” Brokers may access the personal data by public records (e.g., driver’s license, court records, and marriage licenses.)

<u>Statistics on Data Brokers and Identity Theft Crimes:</u>

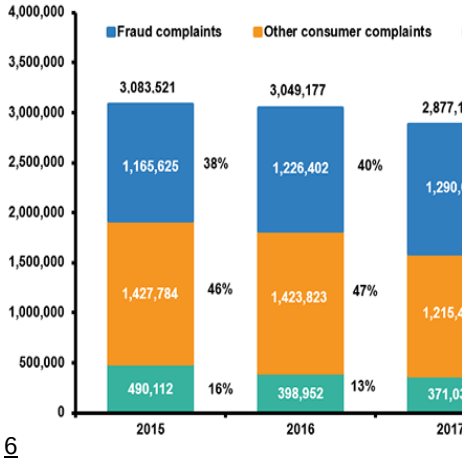


5

fx.com/blog/wp-content/uploads/2015/04/section-1.png.

4- An image on Data brokers and how they access information.

5- A bar graph on identity theft.



6

The Protection of Personal Data:

The UN Global Pulse Initiative has stated the need for consolidating new data sources and the technologies for humanitarian reinforcement. In order to develop the Sustainable Development Goals, the UN finds it necessary that a diligent data privacy and data protection materials, as well as mechanisms should be established in order to certify that responsible data applications are executed from the beginning. Although the surveillance over data privacy and data protection has globally increased, the challenges we face are many. According to the UN Global Pulse Initiative (GPI), these challenges follow from the fractured care landscape and the absence

6 "Facts + Statistics: Identity Theft and Cybercrime." *III*, www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

in materials and developing strategies for privacy, which guarantee that the data may be used safely in the context of a humanitarian or evolution cause.

After the Facebook data breach[7], the UN wants to debate the data protection according to its rules. The UN spokesman for the current UN Secretary-General António Guterres has mentioned that the unsanctioned use of personal data on Facebook should be discussed with all the stake-holders in the industry of information in order to meet the UN prerequisites. Stephane Dujarric, the spokesman for António Guterres has stated that “The debate around the use of personal data —how that is done, the transparency that is needed— is of concern for all of us." The Secretary General of the UN is requiring that the UN will be a place for discussing what further scandals the citizens may be expecting and for finding solutions to these problems together.

8

[7] Murphy, Margi. “Millions of Facebook User Records Exposed in Data Breach.” *The Telegraph*, Telegraph Media Group, 3 Apr. 2019, www.telegraph.co.uk/technology/2019/04/03/millions-facebook-user-records-exposed-data-breach/.

[8] Photos, United Nations Global Pulse. “Day 1i.” *Flickr*, Yahoo!, 28 Feb. 2017, www.flickr.com/photos/132738243@N04/33120520446/.

6- The UN GPI Meeting

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United Nations High Commissioner for Refugees (UNHCR)

The UNHCR is involved in the protection and privacy of refugees' data. A report has been written recently in 2018 on Guidance on the Protection of Personal Data of Persons of Concern to UNHCR.[9] It contributes to ensuring the protection of personal data with the purpose of obliging the personnel of the UNHCR in the implementation and elucidation of the Policy on the Protection of Personal Data of Persons of Concern (DPP), brought in May 2015.

United Nations High Commissioner for Human Rights (OHCHR)

The OHCHR has prepared a report on the privacy in the digital age, after the General Assembly's request regarding resolution 68/167. The report on ensuring privacy was discussed in the General Assembly at its 69th session (December 2014).

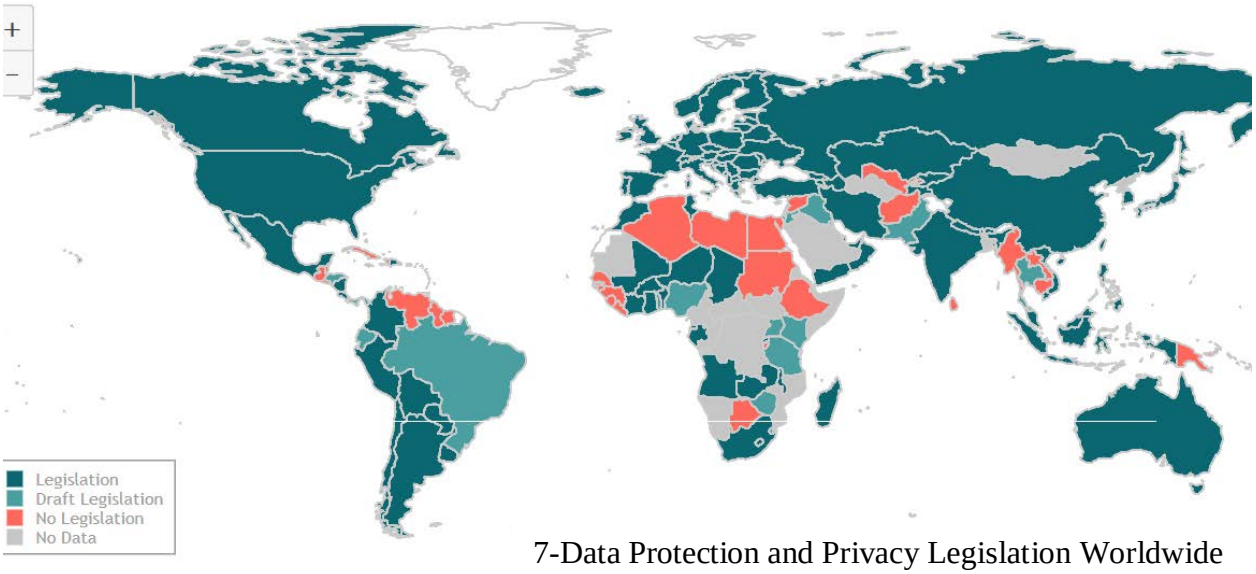
Organization for Economic Cooperation and Development (OECD)

The OECD elaborated its privacy instructions, which included privacy principles and cross-border flows of personal data. Following the project of OECD, the Council of Europe's Convention has begun. The OHCHR further encouraged all parties and organizations to express their views on this issue and report.

[9] www.refworld.org/pdfid/5b360f4d4.pdf.

United Nations Conference on Trade and Development (UNCTAD)

The UNCTAD has gathered facts and numbers on Data Protection and Privacy Legislation Worldwide. The UNCTAD Global Cyber Law Tracker is the first global association of cyber laws. It aims to follow the state of electronic trade prescriptions in the sector of electronic transactions. It further protects consumers encouraging data protection. The UNCTAD has put in place cybercrime legislation with the contribution of 194 member states, of which 107, including 66 developing or in transitional economy countries, have enacted this legislation in order to boost data protection and privacy. [10]



7-Data Protection and Privacy Legislation Worldwide

TIMELINE OF EVENTS

[10] Unctad.org. (2019). UNCTAD | Data Protection and Privacy Legislation Worldwide. [online] Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [Accessed 6 Jul. 2019].

DATE	DESCRIPTION OF EVENT
10 December 1948	The Universal Declaration of Human Rights was associated with the 12th fundamental right for the right of privacy.
1967	The FOA (Freedom of Information Act) is brought up among the member states, and, according to that,, everyone may request access to relevant documents from the agencies of the states.
1983	The Federal Constitutional Court of Germany makes a rudimentary decision on the official count judgment. This verdict is considered very vital for the data protection history.
2013	The European Commission provides Regulation 611/2013 to notify citizens about personal data breaches under Directive 2002/58/EC.
18 December 2013	The United Nations General Assembly adopted the resolution 68/167 named as 'The right to privacy in the digital age.' The UNHCR report pertains to data protection and privacy. The GDPR has replaced the Data Protection Act.
September 10-28 2018 and 2018 generally	The United Nations High Commissioner for Human Rights Treaty A/HCR/39/29 was discussed in the 39th session of the OHCHR. Throughout 2018, The UNHCR report pertains to data protection and

	privacy. The GDPR has replaced the Data Protection Act.

RELEVANT UN RESOLUTIONS, TREATIES AND EVENTS

United Nations High Commissioner for Human Rights Treaty A/HCR/39/29

This treaty was established to provide possible solutions for the data protection and privacy issue.

United Nations General Assembly Resolution 68/167

The United Nations General Assembly adopted the resolution 68/167 called “The right to privacy in the digital age” on 18 December 2013. This resolution elaborated on the negative impact that scrutiny and interceptions of the communications may have on human rights. The committee requested from the UN High Commissioner on Human Rights to furnish possible solutions by writing a report on how the privacy should be protected in digital age.

United Nations High Commissioner for Human Rights Resolution 28/26

In April 2015, the OHCHR adopted resolution 28/16 in the 28th session declaring that there should be a Special Rapporteur on the Right of Privacy for a three-year time. In this resolution, the violated right of privacy

of citizens caused by the arising technology was mentioned and the states were requested to contribute to the Special Rapporteur.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The Global Pulse:

For Data Privacy and Protection, the UN GPI has set:

1. Privacy Research and Innovation —this point requires processing and discussing new methods, substructure, and ways to corroborate the secure and responsible use of Big Data.
2. Responsible Data Advocacy and Adoption —this point aims to alter the international communication on responsible data firms and data access by decreasing the likelihood and increasing the welfare of big data on socializing via policy participations and public events.
3. Operational Privacy and Capacity Building —this point amalgamates privacy rules and laws into a study in the Global Pulse's own data alteration projects. It works together with important stakeholders in order to develop a capacity on the number of responsible data practices for the international humane environment (a successful business.) As mentioned by the United Nations Human Rights Committee as a General Comment 16 in 1988, "The collecting and storing/holding of personal information on computers, data banks, and other electronic devices must be justified by law, whether by public authorities, private individuals or bodies."

The UN GPI has formed a Data Privacy Advisory Group. They have reinforced this group with professionals coming from private and public sectors. In addition, researches, educators and the civil society have taken an active part through an international congress to discuss and cooperate on the topics of using data appropriately, data privacy and data protection with the intent of setting examples and good practices, as well as strengthening the general opinion.

The Data Privacy Advisory Group seeks to inaugurate a global dialogue on protecting data and data privacy, as well as develop serious data studies for humanitarian and development fields on data protection and data privacy. It also raises public awareness with regards to understanding the positive impact of big data for the same development and humanitarian reasons. Lastly, the Global Pulse also encourages everyone to comprehend the challenges and meet the requirements in using responsibly and sensibly the big data for the same purposes. Furthermore, the GPI has set data privacy principles based on the observations and instructions of the Regulation of Computerized Personal Data files presented by the GA in the resolution passed on 15 December 1989.[11]

7- An image of the Global Pulse symbol

<u>The General Data Protection Regulation (GDPR):</u>

The GDPR was enforced on 25 May 2018. The main aim of the organization established by the European Union is to change and organize the manner, in which sectors, businesses and companies manage their data. It further reviews the jobs of the CIO (Chief Information Officer), CMO's (Chief Marketing Officer) in a business. The regulation instituted for the protection of personal data and normal data nourishes the simple rights of the citizens in the digital era and eases work by elucidating the procedures for both public bodies and companies in the digital single market. Its previous attempt has been to set a current single law for all the countries under the European Union. There has also been a Data Protection Law Enforcement Directive in 2016, in which there has been information on the protection and safety of personal data that has a connection with criminals, the removal of penalties, and the free execution of the data.

[11] *UN Global Pulse,* www.onlinevolunteering.org/en/un-global-pulse.

When the directive was enforced on 5 May 2016, the EU countries were required to incorporate it into their national law. This attempt was successful in resolving the issue. The European Union has encouraged the member states to establish national bodies responsible for the protection and privacy of personal data regarding Article 8(3) of the Charter Fundamental Rights.

African Union:

The AU has established the African Union Convention on Cybersecurity and Personal Data protection in June 2014 to set national and regional regulations for electronic transactions, cyber security and the protection of personal data.

POSSIBLE SOLUTIONS

In order to ensure the protection of personal data, there are a few major steps that could be taken with the purpose of tackling the issues arising from it.

1. One major step to be taken for both More Economically Developed Countries (MEDCs) and Less Economically Developed Countries (LEDCs) is the adoption of stricter regulations, which will aim at protecting personal data in a more reliable, safe and cohesive way. This can be achieved with the help of the United Nations and other international organizations.
2. Workshops may be organized by experts for companies in need of safely storing their files and documents without facing issues, such as cybercrime or identity theft. This would especially contribute to a safer storage of personal data.

3. The establishment of national organizations consisting of experts who will control data breaches.
4. Providing clearer and practical information to users of a service.
5. Building an international consensus in regard to the legal age, at which children would be able to use social-media websites.
6. Raising public awareness of the upcoming risks of technology as far as the protection of personal data is concerned.

BIBLIOGRAPHY

UNCTAD. "Data Protection and Privacy Legislation Worldwide." *UNCTAD*, 27 Mar. 2019, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

"The New EU Regulation on the Protection of Personal Data: What Does It Mean for Patients?" *EPF*, www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf.

"The New EU Regulation on the Protection of Personal Data: What Does It Mean for Patients?" *EPF*, www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf.

European Commission. "Data Protection in the EU." *European Commission - European Commission*, 7 May 2019, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

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

"Law on the Protection of Personal Data." *LAW ON THE PROTECTION OF PERSONAL DATA CHAPTER ONE Purpose, Scope and Definitions*, www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf.

"A Brief History of Data Protection: How Did It All Start?" *Cloud Privacy Check (CPC)*, https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/.

"101: Data Protection." *Privacy International*, https://privacyinternational.org/explainer/41/101-data-protection.

Team, WebFX. “What Are Data Brokers - And What Is Your Data Worth? [Infographic].” *WebFX Blog*, 18 Apr. 2019, www.webfx.com/blog/general/what-are-data-brokers-and-what-is-your-data-worth-infographic/.

“GDPR.” *DecisionWise*, https://decision-wise.com/gdpr/.

“The History of Data Breaches.” *Digital Guardian*, 3 Jan. 2019, https://digitalguardian.com/blog/history-data-breaches.

“The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law.” *Taylor & Francis*, www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176.
UNCTAD. “UNITED NATIONS GLOBAL PULSE INITIATIVE: DATA PRIVACY & DATA PROTECTION ACTIVITIES OVERVIEW.” *Global Pulse* , UNGlobal Pulse, Apr. 2016, https://unctad.org/meetings/en/Contribution/dtl_eweek2016_UNGlobalPulse_en.pdf.

“Right to Privacy in the Digital Age.” *OHCHR*, www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

To have thorough information on the statistics check this website:

https://safeatlast.co/blog/identity-theft-statistics/