International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:06, Issue:07 "July 2021"

AN EXPLORATION OF CONTEMPORARY NUANCES IN DATA PRIVACY AND GOVERNANCE

Soham Guha Mazumder

Delhi public school sushant lok gurugram

DOI: 10.46609/IJSSER.2021.v06i07.038 URL: https://doi.org/10.46609/IJSSER.2021.v06i07.038

ABSTRACT

Data in the 21st century has transformed into the most valuable raw material or input resource in any economic, technological or social venture or business. By virtue of data, it has become possible to harness the powers of machine learning, IoT, Data science, and make advancements in AI and research. However, it has been noticed that this hunt for data has led business and data miners to overlook the basic right of people- their privacy. Technological advancements gather a lot of data on people and their associations for many businesses. This has led to unintentional data of people and unjustified use of data to be carried out. Hence it is of utmost importance for a data privacy and data protection framework in modern society. This paper aims to focus on the much needed topic of data privacy, analysing its modern meaning, its need in the present world and various measures of data privacy. We also look at how privacy has been politicized and the various privacy amendments made by various governments across the world. We look at the impact of privacy regulations on innovation in companies imposed by GDPR and other data protection authorities and analyse a famous example of data breach. Analysis in this paper points out that there is a need for awareness and acknowledgment about one's privacy, especially in developing countries. Data privacy at the cost of reduced technological innovation is detrimental, and a holistic approach to both privacy and innovation is needed in today's world.

Keywords: Data, Business, GDPR, Privacy, Government

Introduction

Data privacy, an innovation familiar to most, is encountered in tame forms in a lot of domestic activities such as providing personal information to a website or to just about any platform on the Internet. But the definition of data privacy and its various aspects and functioning have undergone an enormous change with the inevitable technological boom of the contemporary world. It has now been widely politicized and has been integrated with governance to provide rules and regulations that are different in different countries, according to their statutory rules.

ISSN: 2455-8834

Volume:06, Issue:07 "July 2021"

The constituents of data privacy methods as explained by GDPR (General Data Protection Regulation)[1]*are that there are 2 components, data protection, and data privacy. Data protection means keeping data safe from unauthorized access. Data privacy means empowering your users to make their own decisions about who can process their data and for what purpose.* According to this definition, GDPR aims to make data usage completely transparent to citizens and ensure the proper treatment of precious data. One of the major reasons why data privacy regulations have become so essential is- big data, which has, obviously, improved and enhanced the efficacy of business and technological development as well as made personal and domestic life much simpler. On the darker side, big data comes with a negative impact on privacy. With the sheer amount of data big data now procures, it could lead to the unravelling of much more personal data than was intended, due to the network of links between people and their associations. For example, once an analysis of shopping patterns for creating customized advertisements, a department store correctly inferred that a teenage girl was pregnant[2](K Hill, Forbes. inc). Furthermore, data breaches in medical treatment and research could also have devastating effects, personally or publicly. Hence, there is a painfully obvious need for data regulation and regulation in the handling of big data, without losing out on productivity and development. For this purpose, several countries and big companies have made amendments to ensure data protection. Companies are now taking a leap towards privacy, called the '*Big Tech's Shift to Privacy'*[3](Mitchell Noordyke, iapp.org). As said by Google CEO Sundar Pichai, data privacy cannot be a luxury good that only appeals to the rich[4]. In this paper, we have explored the political amendments made by different governments and their impact and present implementation on the public. We have discussed the efficacy of the systems and also the rules and regulations enlisted by big tech companies in granting secure data transfer and privacy and will be discussing some present-day legal and technical ways of data privacy and processing.

Discussion

Firstly, we will talk about the measures taken worldwide, and then we will discuss internal and localized aspects of different countries. The GDPR, although relevant only for EU organizations, has its effects worldwide. GDPR enforces and its regulations require every company in the EU and affiliated countries to comply with the GDPR regulations, aiming to create more consistent protection of consumer data across the globe. It imposes the need to provide consent of subjects for data processing, making data anonymous for identification safety, and providing data breach notifications, to name a few. It contains several laws and articles such as Article 17 which provides consumer accessibility and portability where consumers have full access to what is being shared and can also delete some of their personal data under certain circumstances. Article 35 demands that companies that are heavily dependent on consumer data and processes data

ISSN: 2455-8834

Volume:06, Issue:07 "July 2021"

revealing subjects' private information, appoint data protection officers as a dedicated post that would advise companies on complying with GDPR regulations.[5]

On the grounds of varying cultural and national laws, different countries have adopted different methods for consumer privacy. China's Standing Committee of the National People's Congress published the first draft of its Personal Information Protection Law(PIPL) to the public in October 2020. Alongside existing robust data privacy laws in China, the PIPL also brings several new developments under its belt including steep fines, extraterritorial applicability, laws managing cross-border transfer, and the need for data protection officers. For the UK the story is different. Post-Brexit, due to the severing of the UK with the EU, UK became a third-party country to all members of the EEA (European Economic Area), prohibiting data transfers across borders, until an adequate decision is applied from the European Commission. Brazil also saw its first major data protection law come into force in 2020 after a series of setbacks and delays. This law, being enforced and implemented fully by August 2021 will serve as a testimony for the quality and robustness of the data protection authority of Latin America. Canada's government enacted the Digital Charter Implementation Act(DCIA) on November 17, 2021. This act is meant to override the existing data protection law and introduce new and advanced methods for data privacy including a private right to action and fines that could exceed those of the GDPR.[6]

Needless to say, there is a lot on the plate for tech companies and big organizations in the privacy department. While most of the organizations have not fully attained GDPR compliance, due to lack of resources and constant enhancement of the privacy policy framework, top companies like Google, Facebook, and Amazon have updated their privacy policies to suit the GDPR standards. As privacy becomes a big thing, it is quickly becoming essential for companies to adapt at a faster rate to bring about policies and data protection officers because, in this evolving world, organizations who are compliant with GDPR would likely have a competitive advantage over those who are not[7]. To add fuel to the fire, several countries are adopting GDPR inspired frameworks, as discussed earlier, to localize data privacy laws in their respective countries. Although companies have had a few years to cope with the increasing policies and regulations of the GDPR, the emerging country-wise policies are brewing trouble for tech companies as they struggle with deciding which laws apply to them, which laws to prioritize due to the deadline, and the enhancing breach reporting requirements.[8]

While compliance is key, it can get quite tough to balance compliance with privacy regulations and innovations with a forward mindset. Taking the case of new innovations like machine learning, we are familiar with its numerous benefits and capabilities. But as we saw earlier, there are numerous cases of privacy breaches and uncontrolled applications of machine learning that are not meant to happen. Although companies are adopting methods like de-identification, data

ISSN: 2455-8834

Volume:06, Issue:07 "July 2021"

minimization, and data retention limits, these only benefit the privacy of consumers while falling short of providing adequate productivity in innovation and development. While aiming for holistic development, it is notable that regulation can often boost innovation as well. Early and well-planned compliance can build up trust in consumers which in turn can increase sales and consumer interest. Another approach could be to develop a 'regulatory sandbox. The function of this would be to review and correct any policies and programs with regulators in a controlled environment, this would increase partnership with privacy regulators and would aid in the journey of a new product or service.[9]Let us talk about the recent most famous data privacy breach- the Facebook data breach and the probable causes.

Facebook, one of the world's leading companies and the largest social media sites saw itself in a dire situation in March 2018. The company was caught up in a large-scale data breach scandal, in which the British political consulting firm Cambridge Analytica acquired the personal data of around 87 million users without their consent and used it for political purposes, namely in the 2016 U.S. Presidential elections but also in the Brexit Vote Leave campaign.[10] While the major offender was Cambridge Analytica, some other companies and firms also got hold of private data. The probable causes of this incident could be broad including unenforced safeguard against companies using private information heavily, little to no oversight of developers by Facebook, developer abuse of Facebook API, and users agreeing to overly broad terms and conditions. Cambridge Analytica was able to harvest data using a personality quiz app called this is your digital life. The information generated from this app is useful for building a psychographic profile of users. Adding this app on Facebook enables the creator of the app to view private information as well as all the friends on Facebook.[11] The aftermath of this resulted in Facebook shutting down tens of thousands of apps and many other apps which were using their data inappropriately. Facebook, as well as other firms and companies involved in this scandal ended up paying hefty amounts to the authorities for their involvement and Facebook, adopted a better secure planned action for privacy safeguards.

Conclusion

Although privacy regulations and laws have come a long way from a scarcely implemented concept to an essential and major aspect of all businesses in the modern world of the 21st century, it needs more recognition and improvement to keep up with evolving innovation. Apart from laws and constitutional mandates and technological features to enable data privacy, it is equally important for the consumers to have awareness and knowledge about the product that they are using or the services that they are joining. They need to be aware of AI privacy rules and acknowledge the privacy of their data without overly agreeing to the service's terms. Consumers need to be empowered to question everything and demand their privacy. Shifting the spotlight on

ISSN: 2455-8834

Volume:06, Issue:07 "July 2021"

the situation in India, there is a pressing need for awareness on this topic among citizens. Many of the economically challenged in India are vulnerable to attacks on their personal data without them knowing, hence it is the responsibility of the Indian government to act on this issue and spread awareness about data privacy and the value of one's data. Currently, there exist no particular data privacy acts in India. The only existing act is the IT act which gives grieving individuals the right to compensation following improper use or disclosure of personal information. This is very alarming since technological development is on the rise in India and with that, also the need for an organized pre-planned data privacy framework to avoid data breaches and consumer safety. Presumably, the lack of interest and knowledge about data privacy in citizens could be the reason for the slow approach of the government towards data privacy.

References

1. Ben Wolford (2016) A Guide to GDPR Data Privacy Requirements
2. Kashmir Hill (2012) '*How Target figured out a teen girl was pregnant before her father did*
3. Mitchell Noordyke (2019) 'Big Tech's Shift to Privac
4. The Economic Times, Panache (2019) '*Google CEO, Sundar Pichai on data privacy'*
5. General Data Protection Regulation(2018) [https://gdpr-info.eu/]
6. Andrada Coos (2021) Data Protection Legislation Around The World in 2021
7. He Li, Lu Yu & Wu He (2019) The Impact of GDPR on Global Technology Development, Journal of Global Information Technology Management, 22:1, 1-6, DOI: 10.1080/1097198X.2019.1569186
8. Aleksandra Popova (2020) '*Facing a Privacy Breach Under Growing GDPR-inspired Laws Can Pose Challenges for Companies*
9. RegTech Analyst (2019) '*How Can Companies Balance Compliance with Innovation*
10. Raquel Pita Guerreiro Marcelino Duarte (2020), '*CASE STUDY: Facebook in Face of Crisis*
11. Dan Patterson, TechRepublic (2020) Facebook Data Privacy Scandal: A Cheat Sheet
12. Umesh Kumar, Financial Express (2021) '*Why India is Indifferent to the Data Privacy Issue*

