International Journal of Legal Expatiate Vol 2 (2022) Pg. 1-7 ISSN: 2583-7885 (Online)
Published by Author Lens

"Data Privacy in the Age of Big Tech: Balancing Innovation and Regulation"

-Abhishek Mukherjee*

Abstract

In the age of big tech, data privacy has become a crucial issue. With the increasing amount of personal information being collected and shared online, there is a growing concern about how this data is being used and protected. Balancing innovation and regulation are key to ensuring that individuals' personal data is protected while also allowing for advancements in technology. While government regulation can provide a framework for protecting personal data, it is important to also consider the role of industry self-regulation and consumer education in promoting data privacy. Additionally, it is important to consider the potential impacts of data privacy regulation on the tech industry, including small businesses and startups. Overall, finding the right balance between protecting personal data and fostering innovation is crucial for ensuring the responsible use of technology in the digital age.

Key Words: *Data Privacy, Big Tech, Innovation, Regulation*

Introduction

There have been huge increases in the number of worries over data privacy as a direct result of the rapid growth of technology and the growing power of large technological businesses. It is vital that a balance be found between the promotion of innovation and the protection of individuals' rights to privacy as personal information is being collected, stored, and analysed by these corporations. In this article, we will investigate the problems and concerns that surround data privacy in this day and age of big technology, and we will investigate the role that regulation can play in addressing these problems.

For the last few decades, we have witnessed a paradigm shift in data usage as it has been more accessible and portable. With the advent of mobile devices and digital assistants, many services

* BALLB (Hons.) DSNLU

can be accessed from any place around the world. Some of these services include social media platforms, e-commerce sites, and other service providers like Netflix, Amazon Prime Video, and Hulu among others. However, with this technology is comes an increased vulnerability to privacy invasion that may not only damage user reputation but also their financial status. Such cases are common in some forms of advertisement that have become a normal part of our lives. That makes them a concern to both consumers and companies in the online advertising space whose goals include generating revenue

Despite being one of the leading sources of information on the Internet, the use of internet advertisements has raised significant concerns in public health sectors and consumer protection groups. This is because most advertisements that are targeted at people who would be interested in goods and services are highly unethical and pose serious risks to users' privacy.

This paper examines data privacy issues and how they impact the efficiency of big tech companies in marketing their products through personalization and segmentation of audiences, targeting specific demographics within a region or country, developing ads for a certain demographic, including how those users make decisions on whether or not to purchase the product advertised, where is the actual delivery time and when will it arrive, and how it is received when compared to its original time to market. We also discuss how the issue of data privacy affects small business owners, which they rely on for delivering their products, and finally why big tech should consider using regulation to protect and enforce what happens to consumer data and how this might work against their interests.

Privacy Issues Affecting Small Business Owners

When it comes to matters of privacy, owners of small businesses confront a range of challenges, including those associated with the collecting, storage, and sharing of data. Companies that gather personal information from customers, such as names, addresses, and credit card numbers, have a responsibility to ensure that this information is kept private and is not shared with third parties without the customers' prior consent. This involves putting in place stringent security processes to avoid data breaches, such as encrypting sensitive information and requiring users to log in with passwords. In addition, proprietors of small businesses have a legal obligation to comply with a variety of state and federal laws, including the General Data Protection Regulation (GDPR) and

the California Consumer Privacy Act (CCPA), both of which govern the gathering, storage, and dissemination of personally identifiable information.

The privacy of their employees is an additional concern for owners of small businesses. Employers have a responsibility to uphold their workers' rights to privacy in all aspects of their lives, including their personal lives and actions outside of the workplace. This entails not monitoring the emails, internet use, or phone calls of employees without first obtaining their permission.

In addition, proprietors of small businesses ought to have a transparent privacy policy that details the methods and procedures they follow regarding the collecting, storage, and sharing of customer information. The purpose of this is to educate customers, employees, and other stakeholders regarding the treatment of their personal data.

Last but not least, proprietors of small businesses need to be aware of the potential repercussions of privacy breaches, which may include legal action and damage to the company's reputation. As a result, they need to be proactive and take measures to secure personal data, in addition to being honest about the techniques they use to handle data.

The introduction of new technologies in everyday life has made them available to everyone no matter where they live or how old you are. These technologies are used for multiple purposes, including monitoring location, making video calls and messages, collecting information about customers and their behaviors, storing it in databases, connecting computers, and much more. However, these innovations are opening up opportunities for businesses to collect and store massive amounts of data and at times to exploit such data for malicious reasons. For example, companies have begun tracking users on social media websites to understand their actions and develop personalization features (Kozlowski & Swartz, 2013). Similarly, advertisers now know what users think before buying anything in order to offer the best quality products at desirable prices to attract customers. It is a worrying trend, especially during COVID-19 pandemic, since even companies that provide essential needs are vulnerable to disruption by cyber attacks. Customers are always concerned about the confidentiality of important data and sometimes lack awareness about the amount of control they have over such information. A study conducted by Giannakopoulos et al. (2020) found out that more than 90% of respondents have negative attitudes

towards big tech companies, yet in reality these companies collect large amounts of sensitive information that could easily be used to invade into someone's privacy. Therefore, companies need to put up strict policies that would prevent misusing or obtaining confidential data if they want to remain competitive and retain customers. For instance, in 2017 Facebook introduced "Facebook Ads Data Policy Enforcement" to monitor and report illegal changes in user's profiles (Giannakopoulos et al., 2020). If there is any breach detected this policy would provide users the option to opt-out and delete their data and avoid getting affected by identity theft.

The problem of customer data privacy arises from two main perspectives: internal and external. On one hand, an organization's own data contains only limited information that it uses internally for planning and research, decision-making, innovation and development, employee training, and strategic management. Additionally, consumers' data stored when shopping online are usually anonymous, meaning that people do not know whether or not their data is disclosed to third parties. The second perspective entails the collection of data that is used to train employees to improve their performance or improve user experience via customized advertising. Although both categories of data have different implications to organizations, the former is far more useful than the latter since it allows the company to plan and achieve their goals. Furthermore, this private and privileged insight enables organizations to deliver personalized experiences for users. As per Giannakopoulos (2018), "theoretical frameworks have focused on either individual consumers or corporate clients, but not on individuals as the primary actors" (p. 1). Given that marketers are increasingly sharing information that can be used for better targeting of advertising and other promotional activities with customers as well as employees, the topic of data privacy becomes all the more crucial for companies to address. Moreover, given the fact that many industries such as banking, insurance, healthcare, and transportation (BHT) are already going through massive shifts in consumer behavior due to technological advances, the importance of data privacy cannot be overemphasized. Companies should aim to ensure that their systems are safe so that they do not get hacked by hackers and gain access to valuable personally identifiable information or PII. Otherwise, they risk losing customers and harming their reputations in front of their colleagues.

Data Privacy Issue and Impact to Marketing Performance

Policies that focus purely on preventing misuse of customers' personal information without considering the overall purpose of these efforts could lead to problems. First and foremost,

companies need to evaluate themselves in terms of current regulations and compare with what they are currently doing on similar activities. They need to establish whether they are adequately promoting user privacy while protecting their brand reputation in terms of their competitors. For example, BHT departments rely heavily on Google Analytics and Facebook pixels to measure their success rates. These metrics suggest that if there are a number of conversions going down on Google, it means that website visitors are less likely to stay longer on the page. Consequently, this indicates that marketers are becoming less effective at reaching their target audience. Thus, creating effective strategies to combat this issue is imperative. When analyzing the effectiveness of existing approaches to regulating data privacy on behalf of marketing managers, researchers point out several limitations that may prevent companies from achieving their potential. From a theoretical standpoint, scholars have come up with various ways of addressing the issue, although none of them will truly help in resolving the dilemma. At first glance, one may argue that privacy as a concept is largely irrelevant to marketing executives since they focus solely on the consumer. Nevertheless, as soon as a person opens his pockets and pays attention to the ads being served to him, he becomes part of the system. He voluntarily gives consent to advertisements he sees online, which translates into his active involvement in marketing processes and actions aimed at improving or affecting the outcomes of the commercial. Researchers point out that the process of establishing user privacy does not necessarily imply that people are happy with the measures taken to block their access to their personal information in favor of those that protect their privacy. Instead, the problem lies in the way information services collect data about customers, use it to customize their products, and sell data to third parties without their permission.

Researchers have argued that it is extremely impractical to ban collecting and saving data from browsers because this approach would violate basic standards of freedom of expression and human rights. Indeed, there is evidence that shows the practice is actually hurting society as users of free services who willingly agree to share information may lose trust in social networks where they spend so much time. In this case, companies will continue collecting information, and that is why there is no consensus as to the right way forward. Overall, privacy should not be seen as something that belongs to users only. Rather, it needs to be treated as a collective interest as opposed to an individualistic pursuit. As mentioned in this section, the issue is critical for today's fast-moving economy that keeps evolving by leaps and bounds. People constantly seek unique items that they find exciting and unusual. They want to learn about unfamiliar things that exist in the real world.

To succeed in such ventures, they need to communicate, feel connected, and share knowledge with others by staying updated on news and events happening in their immediate environment. Unfortunately, though, companies still rely on third party services that gather information about users of websites without first asking them for their permission. Ultimately, they may miss opportunities and fail to reach their target audience. This is an alarming trend considering how technology has advanced rapidly in recent years, and it will certainly affect other aspects of daily life. Organizations must pay close attention to the manner by which they collect, store, and act upon different types of customer information to meet their respective objectives.

Data Privacy Issues and Impacts on User Decisions

In order to effectively meet their aims, companies need to analyze the patterns and trends that exist among their users. By doing this, they can determine which ones are actively engaged with their phones and other electronic devices and in what context. For example, if there is a sudden surge in sales during holidays or particular seasons, then marketers would be able to predict what the upcoming season will look like and therefore focus their resources and effort on those campaigns. Likewise, marketers can conduct surveys to see which regions of the population receive the highest traffic. They will get a glimpse of potential markets and then devise creative solutions to increase the likelihood of turning out loyal customers. After gathering this information, marketers would have enough data about their customer base to build plans based on their preferences and the trends that arise in them. Having this data helps marketers focus on the segments of their users that generate the most profit and subsequently attract potential customers. This strategy works because the competition between brands for customers has intensified significantly over the years. Even though major corporations have high profits, many niche players struggle to compete with bigger rivals as a result of low pricing and poor customer support. In order to maintain their popularity among their existing and future customers, these companies must continuously innovate and evolve the level of interaction.

Conclusion

In conclusion, maintaining data privacy in this day and age of big technology is a difficult challenge that calls for a finely tuned equilibrium between innovation and regulation. On the one hand, large technology businesses are a primary driver of innovation and economic growth, and

the data-driven business models that these companies employ have the potential to enhance the quality of our lives in a myriad of different ways. On the other hand, the enormous volumes of data that these firms acquire and the manner in which they use that data present significant privacy concerns. The development of data privacy legislation that are not only effective but also flexible, and that take into consideration the one-of-a-kind characteristics of the digital age, is the critical component in achieving the optimal level of equilibrium. Because the internet does not recognize national boundaries, these policies ought to have a global scope as well. In the end, the goal should be to create an environment in which large technology businesses may continue to innovate and flourish while simultaneously respecting the rights of individuals to their own privacy.