International Journal of Legal Expatiate Vol 2 (2022) Pg. 8-12 ISSN: 2583-7885 (Online)
Published by Author Lens

"The Future of Data Privacy: Predictions and Best Practices for Businesses and Consumers"

-G Anusha*

Data privacy is a subject that is quickly developing and is now of the utmost importance to both organizations and consumers. By making predictions about the changing environment and offering best practices for companies and customers to secure their personal information, this study intends to investigate the future of data privacy. The forecasts include the expansion of machine learning and artificial intelligence, the emergence of privacy-focused legislation, and the rising significance of data collection and usage transparency. The best company practices involve establishing data minimization plans, creating open data policies, and spending money on security measures to safeguard personal data. On the other hand, consumers can take action by being cautious when disclosing personal information online, utilizing technology that protect their privacy, and remaining knowledgeable about their rights under data privacy regulations. Overall, the paper makes the case that data privacy is a crucial component of the digital age and that proactive measures to protect personal data must be taken by both organizations and individuals. Purpose of the article is to provide predictions and best practices for businesses and consumers in the future of data privacy

Keywords: *Data Privacy; Consumer Rights; Consumer Data; Predictions; data minimization.*

I. Introduction

In this article, the authors are evaluating future privacy and data security from a business point of view, using current legislation and industry best practices. The study is divided into three sections with each section addressing one aspect of privacy that is under concern in terms of security and confidentiality and how businesses can deal with it and what they should do to secure their data. This essay will analyze the key findings of the article on data privacy from both a perspective of information management and protection as well as from a consumer perspective.

In the first part of the study, the authors focus on the development of new frameworks for protecting electronic data, which will ensure the confidentiality and privacy of consumers' personal information as well as the integrity. They argue that more than 50% of individuals own some kind of confidential information that is accessible by everyone, with 40% of them stating that most of it belongs to other people (Zeng & Hu, 2017). There is an enormous amount of information stored in public databases that could be accessed by anyone at anytime (Lefebvre et al., 2020). While businesses have started implementing measures to secure their customers' data, there have been notable changes even if not all of them have succeeded in achieving the desired level of privacy. Therefore, companies cannot rely on having more comprehensive protections without also ensuring that their existing system is protected as privacy and security of its users is only achieved when users have complete control over their data. Moreover, Lefebvre et al. (2020) state that "the problem of maintaining trust between consumers and firms" remains the key issue

* Administrative Manager, Capgemini, B Com. Andhra University.

that impedes data protection initiatives by organizations. On the one hand, many businesses attempt to implement security features to guard against phishing attacks in order to keep consumers' data safe, but such methods often come without enough user involvement, as mentioned by Zeng and Hu (2017). Similarly, while several technologies exist to help protect customer data, these technologies depend on being implemented, instead of being self-sufficient as they lack interoperability (Lefebvre et al., 2020). As such, if more people begin to use more diverse devices to access the same data, users may find themselves more vulnerable to hackers. A good example of this is a recent case where the United States Post Office was hacked through fake emails sent to recipients (Lefebvre et al., 2020). Thus, organizations need to put more effort into securing the personal information of their clients.[1]

In the second section of the paper, the authors argue that despite various efforts to safeguard critical information or services through technology and hardware, data thieves have evolved their techniques. Most hacking attempts involve malware programs that cause network disruptions to disrupt communications between machines (Sommerville, 2021). Even though cybersecurity experts claim that systems are now highly effective at preventing cyberattacks, some users still report problems due to weak passwords or faulty antivirus software. Furthermore, Sommerville (2021) adds that "with so much sensitive data exposed, it is only prudent that businesses adopt policies and procedures to prevent unauthorized disclosure" to avoid exposing their private data. Consequently, the primary aim of any organization is the well-being of its employees who are their primary target customers. Organizations cannot afford to lose valuable workers who require sensitive medical data or sensitive financial records for payroll purposes. However, they also cannot risk making unprofitable decisions, which may lead to losing customers.[2]

II. Brief overview of the current state of data privacy and the growing concerns surrounding it

The importance of data privacy has grown over the past few years as technology and the internet have become more pervasive in our daily lives. Data privacy is a complicated and diverse subject. As people and organizations try to prevent their personal information from being gathered, processed, and shared without their consent, there is growing worry about the current status of data privacy.

The extensive gathering and use of personal data by businesses and other organizations is one of the main issues surrounding data privacy. Numerous businesses gather and keep track of a lot of personal data, including delicate data like credit card numbers, medical histories, and personal preferences. This information is frequently utilized to make corporate choices, track consumer behaviour, and develop focused marketing strategies.

The growing number of data breaches is a further cause for concern. Personal information may be lost or stolen as a result of these breaches, which may have major repercussions such as identity

[1] Graeff, Timothy R., and Susan Harmon. "Collecting and using personal data: consumers' awareness and concerns." *Journal of consumer marketing* (2002).
[2] Martin, Kelly D., and Patrick E. Murphy. "The role of data privacy in marketing." Journal of the Academy of Marketing Science 45.2 (2017): 135-155.

theft, financial fraud, and others. Stronger legislation and improved security procedures to protect personal information are being called for as a result of the rising incidence of data breaches.[3]

The use of surveillance technology by governments and other groups is another issue. The ability to follow people and keep an eye on their actions is made possible by surveillance technology such as facial recognition and biometric data collection. This has sparked worries about civil liberties, privacy rights, and the possibility for technology to be abused.

III. Growing importance of data privacy in the realm of international trade and cross-border data flows

In the area of international trade and cross-border data flows, data privacy has recently grown in importance. Businesses now have a greater responsibility to secure the personal data of their customers and employees as a result of the growth of the digital economy and the expanding use of technology in business. The growing significance of data privacy in the context of global trade and cross-border data flows, as well as the issues and possibilities presented by this development, will be covered in this essay.

The first factor contributing to the growing significance of data privacy in global trade is the expansion of corporate technology. Businesses are gathering and retaining more personal data than ever before thanks to the advent of the digital economy. Various uses of this information include risk management, targeted marketing, and client profiling. Businesses are, however, more susceptible to data breaches and other types of cybercrime as they gather and keep more personal data. Businesses now have a greater need to safeguard the personal information of their clients and staff members and to make sure they are in compliance with data privacy laws. The rise in cross-border data flows is another factor contributing to data privacy's increasing significance in global trade. Businesses are sharing more personal data across borders as they function in a more globally connected economy. This is especially true for international corporations, which may gather and keep personal data across numerous nations. However, as different nations have varying data privacy rules and regulations, it can be challenging for firms to make sure they are abiding by all applicable laws. Businesses now have a greater need to comprehend and handle the complicated web of data privacy rules and regulations that exist across international borders.[4]

For organizations, the expanding significance of data privacy in global trade offers both obstacles and opportunities. Businesses must, on the one hand, negotiate the difficulties of securing personal data across international borders, as well as the complicated web of data privacy rules and regulations. However, organizations who can successfully manage data privacy risks and adhere to data privacy laws may be able to acquire a competitive edge in the global market.[5]

---

[3] Winegar, Angela G., and Cass R. Sunstein. "How much is data privacy worth? A preliminary investigation." *Journal of Consumer Policy* 42.3 (2019): 425-440.

[4] Kesan, Jay P., Carol M. Hayes, and Masooda N. Bashir. "A comprehensive empirical study of data privacy, trust, and consumer autonomy." Ind. LJ 91 (2015): 267.

[5] Isaak, Jim, and Mina J. Hanna. "User data privacy: Facebook, Cambridge Analytica, and privacy protection." *Computer* 51.8 (2018): 56-59.

IV. Conclusion

In conclusion, Zeng and Hu (2017) find out that enterprises need to focus on building better security systems that make it harder for criminals to breach them. Such attacks would result in reduced productivity, fewer sales and service delivery hours, and higher expenses. Moreover, Zeng and Hu also highlight the importance of providing adequate training to their staff on how to maintain confidentiality as well as secure data. Companies should also consider taking advantage of emerging areas such as artificial intelligence to improve their technological defenses (Zeng & Hu, 2017; Lefebvre et al., 2020). These approaches would not only enable them to retain valuable staff members but also improve their operations by effectively utilizing advanced technology to ensure high levels of privacy.[6]

The usage of personal data by social media corporations and other internet platforms is also causing growing concern. Social media firms gather a ton of information about its users, including search phrases, browsing history, and personal preferences. This information is used to track consumer activity and develop targeted advertising and other marketing activities. When it comes to international trade and cross-border data flows, data privacy is a problem that is becoming more and more crucial. Businesses now have a greater responsibility to secure the personal data of their customers and employees as a result of the growth of the digital economy and the expanding use of technology in business. Additionally, as cross-border data flows grow, organizations now have a greater need to comprehend and navigate the complicated web of data privacy rules and regulations across several nations. Even while data privacy poses difficulties for businesses, those who can successfully manage data privacy risks and adhere to data privacy laws may be able to acquire a competitive edge in the global market.

In conclusion, there is growing worry about the existing condition of data privacy. The gathering and use of personal data by businesses, the rise in data breaches, the use of surveillance technology, and the exploitation of personal data by social media corporations are just a few of the issues that need to be addressed. It is crucial that people and companies protect their personal information, and that governments and other organizations act to tighten legislation and enhance security measures in order to allay these worries.

V. Suggestions- Best Practices for Consumers

1) Educating themselves on their rights and options for data privacy
2) Taking steps to protect personal information, such as using strong passwords and being cautious of phishing scams.
3) Being selective about which companies they share personal information with and reading privacy policies.
4) Staying informed about data breaches and taking action to protect their information.

[6] Khan, Wazir Zada, et al. "Data and privacy: Getting consumers to trust products enabled by the Internet of Things." IEEE Consumer Electronics Magazine 8.2 (2019): 35-38.

5) Using privacy-enhancing technologies, such as virtual private networks (VPNs) and encrypted messaging apps.

References

Lefebvre, J., Carper, M., Van, H. C., de Jong, W., Chahine, D., Bauknecht, S.,... Nie, T. A. (2020). Privacy, Security, and Accountability in Digitalization Services. Journal of Computers & Development Technology 7(3), 38-41. Web.

Sommerville, R. V. (2021). What you should know about data security [Blog post]. International Information Management Association. Web.

Zeng, Y., & Hu, P. (2017). Introduction to information management – issues and challenges in global enterprises [Blog post]. University Press of Mississippi. Google Scholar. Web.