**Class Activity**

**Name: Saman Khan**

**ID: 19K-0354**

**Section: H**

**Data Privacy in India**

The government of India is reportedly planning to pass the Personal Data Protection Bill DPB, which would regulate the gathering, utilizing, transferring, securing, and disclosing of citizens' private information. Despite DPB's regional focus, it represents a significant advancement for global management. By 2022, analysts predict India's digital economy will be worth $1 trillion, drawing a slew of multinational corporations that must adhere to DPB's regulations. Instead of adopting the isolationist framework of Chinese regulation, which forbids global players like Facebook and Google from operating within its borders, India has adopted the EU's General Data Protection Regulation GDPR in allowing global digital companies to conduct business under certain conditions. However, the DPB in India has more protections than the one in the EU. India, as a nation state, would protect the data produced by its citizens as if it were a national treasure, keep it secure within the country's borders, and use it to further India's national security and other national interests. The DPB contains several elements that will necessitate new approaches to business and new ways of thinking about how to run a company. Having to deal with all of them will increase overhead and complicate operations. The points we provide here are meant as a primer for what businesses should think about in light of India's new rule and the rise in data protection regulation globally. Insight into these concerns will aid digital businesses in making strategic decisions about market entry and departure, as well as compliance with future legislation. The Right to Personal Secrecy the Indian Supreme Court determined in 2017 that individual privacy is a fundamental human right. However, every individual leaves a digital footprint that can be traced back to them. Through regulating the gathering, securing, storing, selling, and using of these data, DPB hopes to defend and safeguard the privacy rights of its citizens. Many digital companies lose money providing free services but hope to profit from the sale and exploitation of their customers' personal data, thus any new regulations would have an impact on their cost-benefit calculations. If digital companies can't capture, use, hold, and sell user data as profitably as before, they may need to reevaluate their business strategies. Consent of user under DPB, a digital corporation can't acquire users' personal information without their knowledge and consent. This requires detailing the scope and goal of the data collection. Each subsequent step in processing the data also requires explicit approval. Because digital corporations not only gather personal data, but also process that data to create new information that does not belong to the original user, ensuring compliance with this condition may be difficult. Companies like Uber and Amazon use data analysis to learn about traffic patterns and customer satisfaction, respectively. In addition, raw data might be sent to a data processor for analysis, allowing for the generation of new information in conjunction with data collected by other parties. Businesses will need to reevaluate their current methods of data collection and security, as well as determine whether, when, and how to ask for user consent. When digital enterprises take on the obligation of gaining user consent for both the collection and subsequent processing of user data, they transform from data collectors to data fiduciaries under the DPB. Data privacy and ownership DPB suggests, in theory, that the data source should be the one to claim ownership of their own private information. While not complicated in theory, this approach has the potential to place a significant implementation burden on digital businesses. One can demand the restitution of their property in the real world. When a user asks deletion of all of their information after cancelling their Facebook account, for example, digital companies like Facebook would need to find out a way to comply with this need. In addition to considering how they might utilize the information internally, digital businesses must consider the possibility that they have sold the data to a rival company. There are three distinct kinds of information. DPB has found three types of information that can be used to pinpoint a principal. Information on one's finances, health, sexual orientation, genetics, transgender status, caste, and religious beliefs all fall into the category of "sensitive data." Information deemed extremely vital to the nation's defense or safety falls under the category of "critical data," which is defined by the government. The remaining information is contained in the third, unspecified category. Data Protection Board mandates that data custodians adhere to class-specific guidelines for data storage and processing. Keeping all of your most private and vital information on servers in India is a must. The processing of sensitive data can take place outside of India, but it must be transported back to India for safekeeping. Important records are strictly off-limits for export. For generic information, no limits apply. These days, digital businesses may be found anywhere in the world thanks to the ease with which data can be sent, stored, and processed online.