Data Privacy Protection From Government, Business And Individual's Perspective

Data privacy is defined by Techopedia as information that contains private and usually personal data about an individual. (Techopedia) Being able to properly and secure this data is an important factor that the government, business and individuals that must be considered and be taken seriously. This is because the data stored contains personal information that is highly confidential and with today's technological advancements this data have become more and more vulnerable to threats of unauthorised access by hackers and other activities that would otherwise prove illegal. As such rules and regulations have been introduced so that we are all protected when providing personal details in every transaction that requires us to give out personal information. Personal data and other records (whether medical or financial) are usually collected by many organisations in order to improve their service, advertise or to help identify individuals as quickly as possible. They are an important part of our today's society that is required by the ongoing technological advancements that is happening around the world. Data privacy management requires each and every one of us to play an important role and responsibility towards maintaining our privacy information in check whether it's from government, business and or individual's perspective. Not being able to do so, may result in serious consequences or jeopardise an entity.

Firstly, the government has a critical role to make sure that only those with authorised access can view an individual's personal data. According to (Bennett 2009) the concept of [data privacy] is fused with data protection, which interprets privacy in terms of management of personal information"(Bennett 2009). The Privacy Act 1988, regulates how organisations and individuals handles personal information that helps identify a person. This could be through a phone number, signature or date of birth, all of which are personal details. Under this law outlines the Australian Privacy Principles (APPs) that covers all relevant information that must be followed. (Australian Government, Office of the Australian Information Commissioner, OAIC). The Privacy act 1988, acts and enforces the guidelines to which an extent of whether an individual can maintain "anonymous or using a pseudonym where necessary" (OAIC). The government sets out the data security standards that many businesses and individuals has to follow so that they are protected and in control of the usage of their information. They also educate the community regarding privacy issues, undertake investigations and also develop legislations that will ensure the security of data. The government is the governing body that allows all this to be successfully enact throughout Australia. They acquire data for the sole purpose of identifying an individual so that they can provide the proper service when necessary.

Secondly, businesses must make sure that they are complying with privacy laws and etiquettes regarding the handling of data. According to General Data Protection Regulation (E. Marshall, 2018) "the ready availability of cheap data storage has created a situation where companies can store … [and stockpile] data" which has become a strategy for a range of companies. (E. Marshall, 2018). This data can be a valuable asset for many businesses as data collected can be used for the purpose of advertising, providing better service and identify its market diversity so that they can become more competitive than its competitors. In Accordance to GDPR guidelines (E. Marshall, 2018), businesses must ensure that their use of customer's data must be 'lawful' and indicate the sole purpose of data gathering to the individual. (E. Marshall, 2018)

They must also make sure that the data is secured properly and only those with authorisation can access the data. Businesses must commit towards developing a “clear and updated privacy policy”. (Australian Government, 2018) Customers trust that their personal data and financial data is kept safe by them when they are provided with goods or services. Any breaches or leaks of data from businesses can be costly and may even result in legal actions, loss of trust from customers but most importantly can damage their overall reputation. That is why, it is also their responsibility to have appropriate breach protocols and action plan should a situation like this may arise.

Thirdly, while we can’t control the outcomes from third party safety protocols on data privacy, individuals may stride to develop their own safety system so that they can protect themselves by setting up passwords and being careful online whenever you’re on social media or purchasing goods or services on online platforms. Developing a password that isn’t too ‘predictable’ is one way that you, yourself as an individual can do. By using longer passwords and random letters and number combinations can make it hard for anyone to access your information. Being on social media can also make an individual vulnerable to random pop up ads that requires you to sign up to their services or purchasing goods, that is why it’s really important that research on the companies should be done to make sure that they are legitimate and can keep your information safe. (N. Lord, 2019). It is also the individual’s responsibility that they constantly update their protection system which can be simply as changing passwords every 3-6 months. Being careful on what you do online can really make a difference in achieving and developing a safer system that will keep your personal information safe. (N. Lord, 2019)

In conclusion, in order to achieve a safer protection of privacy data, the roles and responsibility of the government, businesses and individuals must be shared amongst them and each plays an important role so that our personal information are being protected and trusted. Data collection is a way for many businesses and government body to help improve services, to identify market diversity but most importantly help identify individuals through the use of personal information. Keep in mind that failing to follow the privacy policy and laws can result in serious consequences. Our society is constantly changing and technologies are evolving rapidly which makes us vulnerable to attacks and unauthorised access from hackers, that is why we need to constantly adopt towards developing better systems to protect ourselves online. Thus making our future uncertain and full of doubts on the issue surrounding data privacy and protection.

References

1. Bennett, L. (2009). 'Reflections on privacy, identity and consent in on-line services.' Information Security Technical Report 14(3): 119-123.
2. Australian Government, Office of the Australian Information Commissioner, OAIC. The Privacy Act 1988 (Australian Privacy Principles), https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
3. Marshall, GDPR, 2018. General Data Protection Regulation- GDPR: data security is the responsibility of companies by Emmanuel Marshall on 03 July 2018 09:50:06 AEST https://www.mailguard.com.au/blog/gdpr-security-responsibility
4. Australian Government, 2018 Protecting your customers' information -Last Updated: 15 August 2018 https://www.business.gov.au/risk-management/cyber-security/protecting-your-customers-information

5. N. Lord, 2019. 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2019 by Nate Lord on Wednesday May 15, 2019https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe
6. Techopedia. Information privacy- - What does Information Privacy mean? https://www.techopedia.com/definition/10380/information-privacy