
Digital Privacy In Australia Compared To Other Countries

Privacy is the right of an individual or a group to make themselves secluded and express themselves and their information selectively. The concept of digital privacy can be best described as the protection of the information of private citizens who use digital mediums. It is the freedom or right to determine how private information is stored and used. It directs to the desire of people to control or have some form of influence over their data. Digital privacy is the encompassing of information, communication and individual privacy mainly stored on digital platforms. Communication privacy means that message and communication can be accessible only by the sender and the intended recipients.

In the context of the modern world, almost every daily activity in our daily life leaves a digital footprint in some random spots. From GPS tracking and location, cardless payments, smartphone activities, social media platforms, and others thousands of applications allow a seamless digital footprint of our activities about what we are doing, where we are doing and with whom we do.

If we consider Australia, citizens care about their personal privacy a lot. They use the services provided and are aware of the value in terms of personal digital information. Due to a busy lifestyle, they spend less time worrying about their personal information being used. They totally rely on the government and internet service providers for protection and right the use of their personal information. They are not concerned about their personal information being stored and sold to someone else. This is due to the fact that people believe that the information and their activities are useless.

Why is privacy such a big thing to discuss? If we consider an internet flight ticket booking site, the smart algorithm analysis our interest. The information like destination place, time of travel, time of the year are collected. The cookies are stored. Next time when we visit the site again the price goes up significantly. This is how they store our data for their benefits.

Now if we talk about supermarket giants like Coles and Woolworths's loyalty programs, our purchase data is collected every time we swipe the cards. Each swipe of customers' card shows information about the items purchased, quantities and most purchases good. Through this big data, third party business can use that and come up with a new kind of similar products. For those third party companies, these data from Woolworths and Coles have a high value. So, everyone must be aware that those kinds of information exchanges. The consumers must read the privacy policy act when they sign up with these kinds of programs.

During the last couple of decades, there has been a huge development in the technical field. Generation X was the population that was not aware of any technical advancement. Generation Y had a bit of knowledge, but the revolution came in the age of generation Z. People became aware and grew up with the technology. In today's time, society can be classified into two categories as technology natives and immigrants.

Social media stores huge information from its users. Online stores analysis our habits and interests and use that data for various purposes like advertising. We share almost everything

happening in our daily life in those media. From breakfast, we eat, place we travel, a friend we spend time with and a lot more.

Talking about Facebook, it stores our friends and family details. We share single events and stories with people near to us. We share their personal information. I.e place we work, place, we live, the place we study. From these activities that we post on social media a lot of information can be collected and analysis user patterns. For example, researchers at the University of Cambridge successfully used facebook likes to identify not only personality but gender, political affiliation, sexual orientation, and religious affiliation. This can be scary when used in an unfair manner.

Now google is home to all of those things, they keep track of places we live, work, study, and our visit. They know how many times you have visited certain websites and what time we too, also personal preferences and habits.

Based on research conducted on internet users, individuals with profiles on social networking websites have a higher risk-taking attitude in comparison to those who do not; also greater risk-taking attitude exists among men than women.

The digital rights and governance project at the University of Sydney conducted a survey of 1600 Australians about their digital rights, the need for Governance and the responsibilities of social media platforms. The following are the finding of the survey.

Australian personal and professional lives are being transformed by digital disruption, while lawmakers, technology elites and corporate Boards fail to keep up. Based on the survey 67% of citizens can step to protect online privacy but 38% only to feel in control. 80% of the city doesn't want to know what information of theirs is being used by whom, while 26% believe it is acceptable for employers to look at a public social media posts, only 20% say it is acceptable for them to do so when the posts are tagged as private. These numbers show the Australians are seriously concerned about their digital privacy.

The Australian privacy act 1988, defines personal information as “information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual or an individual who is reasonably identifiable.”

Most of the Australian say online privacy is beyond their control. They don't think that they are the one who has access to control the flow of their information.

“In Australia, no jurisdiction has enshrined in legislation a cause of action for invasion of privacy; however, the door to the development of such off causes of action at common law has been left open by the high court in Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (Lenah Game Meats)”

The failure of Australian (FOI) laws to live up to their promise and to the experience in other jurisdictions significantly focus the government's decision-making process.

The level of privacy is different based on personality. Privacy is always a personal preference. No one wants an unauthorized personal to know about their life. Personality with high ranks like military generals, politicians, actors are concerned for wide majority of people. Time and again

we hear the news that the social media account of these personalities been hacked, or some government secrets are leaked. Protections of their information is very essential. Not only these personalities are essential, everyone's privacy should be respected and protected.

It is the government's responsibility to protect a citizen's information. The government must provide protection of citizens' information because citizens put their trust in the government blindly. Privacy acts must be updated regularly because technology is evolving day by day. The information and communication sectors are evolving on a daily basis and the government must be updated with the changes. The government should also ensure that internet service providers are not collecting user data and selling to the third party. It has to make rules regarding storing and using customer data for a better experience of the user.

In China, Chinese citizens are satisfied with their information protection laws because their government keeps track of everything about them and doesn't disclose to any organization.

An individual should also have some sort of responsibility for the protection of their own information. They must be aware of privacy terms and conditions before signing up for any sites or platforms. An individual can protect themselves by applying some safety habits like visiting the trusted sites, using antivirus software, downloading authentic and secure contents from a trusted supplier, turning site cookies off for unwanted and unsafe sites and virtual machines.

Comparing Australian government privacy acts with the European country act, there are some differences. The directive outlines of non-EU countries must adopt privacy legislation of equal restriction and to be allowed for exchanging personal data with only EU countries. Furthermore, companies in non-EU countries must adopt privacy legislation of equal restriction as provided in a Directive. In order to do business with companies established in EU countries. The general data protection Regulation is the recognition of a "right to be forgotten", it requires any group that collects data on individuals to delete the data related to that individual upon the request. The regulation was influenced by the aforementioned European Convention on Human Rights.

The council of Europe, addressed privacy protection regarding the internet in the year 1998 when it published, "Draft guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highway, which may be incorporated in or annexed to Code of Conduct."

Every country has its individual privacy-related acts and law. Protection of citizens privacy is their primary responsibility. There should be standard protocol for sharing information with the authorized authority. Citizen information should only be used for citizen's benefit and they must be aware of it.

References

1. Australian Broadcasting Corporation V Lenah Game meats Pty Ltd [2001] HCA 63, 208 CLR] 199 (15 November 2001) (Australia)
2. Paterson, Moira --- "Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State" [2005] PrivLawpr 20; (2005) 11(7) Privacy Law and Policy Reporter 203.
3. Krasnova, H., Gunthar, O., Spiekermann, S et al. IDIS (2009) 2: 39-63

<https://doi.org/10.1007/s12394-0090019-1>

4. Fogal, Nehmad "Internet social network communities: Risk-taking, trust, and Privacy concerns", Volume 25, Issue 1, January 2009, Pages 153-160, Computer in Human Behavior
5. France, Robert "Privacy in the digital age: a review of information privacy research in the information system", Volume 35 Issue 4, December 2011 Pages 1017-1042, Society for Information Management and the Management Information System Research Centre Minneapolis, MN, USA
6. Al Bareeq, J.M., Aal, A.A, Abozenah, H., Alhourani, D., Alsowaidi, A., Corbally, M., Fadel, E., Sharif, O., Skowronski, S. and Tierney, E. (2017) Research and Ethics for the Medical Profession, Partridge Publishing Singapore.
7. Beecher, MD And Henry, K. (2017) Ethics and clinical research. In Ethics and Medical Decision-Making (pp. 3-9) New York: Routledge.

edubirdie.com