

---

## The Ineffectiveness Of Australian Privacy Laws

In the current world, technology is used so widely and by so many. It assists in a variety of daily tasks such as communication, work and even education. It interconnects our world with the click of a button allowing information to be sent around the world instantaneously. Although allowing the ability for connection, the thousands of terabytes of private information on individuals held by technology and different companies raises the dangerous issue of privacy. While Australian privacy laws cover certain aspects of privacy they have had little effect in protecting an individual's rights in relation to it. This is because laws are becoming outdated due to technological advancements, the people creating these laws don't have a suitable understanding of these advancements to create protective laws, private information is being hacked and abused by companies, and some legislation created has breached the rights of individuals.

With technology constantly changing, reforming laws becomes difficult as the law is reactive to changes, meaning that Australian laws have often been highly ineffective. As technology upgrades, there is a lag between laws as the features and uses cannot be fully understood until the actual technology and its social implications are fully understood. The constant advancement of the internet allows more and more information to be shared around the globe no matter your location, which opens up a wide gate for online attackers. This ability has become a growing problem due to online communication apps and online trolls interfering with people's lives in a way the law refuses to admit. This can be seen through the statistics of suicide rates due to cyberbullying, with one in five Australian children now victims of online abuse, and an average of eight young Australians taking their lives from it each week. The law implicates a punishment for it, yet it is still a growing problem. From the time of introduction of these applications, the lag time for legislation is fatal, pushing for reform to implement effective laws. The loopholes and extensive mass of this problem is something that suppresses the effectiveness of Australian law in protecting these individuals from privacy breaches of this sort.

The ease of access presented by the abyss that is the internet also opens up the ability to commit fraud over a person's identity. Privacy laws already state that this is a crime, but due to the technological advancements of the internet have fallen behind in how to effectively handle it. A woman named Julie had her identity stolen from her driver's licence in 2017 resulting in thousands of dollars of loans being taken out by someone else. As the case got brought to court it was stated that even though the banks had teams dedicated to fraud, the money was leant without adequate proof of identity, just a driver's licence number. The Australian Federal Police said each year people lost hundreds of millions of dollars through ID fraud proving that regulations put in place are not effective in protecting these individual's private information.

Those who create laws are professionals in legislation. Due to this, a comprehensive understanding of the complicity held within technology is inapplicable, making laws to protect individual's privacy from the capability of technology impossible and ineffective. There have been multiple cases where information has been abused under the radar from this lack of understanding such as the hacking of the Australian national university. An individual gained unauthorised access to 19 years' worth of student and teacher information in 2018 with approximately 200,000 people being affected. It went undetected from the end of 2018 to May

---

2019, after the public was assured no data had been stolen, only to be detected when trying to fix the system that allowed the attack to occur. It is found that this level of uncertainty and detection time is not an unusual occurrence. A study conducted in 2018 found that cyber intruders go an average of 196 days without being detected resulting in attackers having around half a year to collect data, monitor an organisations operation, as well as cover their tracks. In addition to this, it takes a further 70 days to respond to the threat putting an enormous strain on thousands of individuals private information. This case resulted in the enforcement of the rule that companies had to inform those whose information was involved as soon as a breach is detected. Privacy laws could not account for the correct protection of this information or the serious nature of the hacking therefore have not been able to effectively protect the privacy of individuals.

A further reason why laws have not been effective in protecting individual's rights is that private businesses have been accessing individuals' private information for commercial purposes, without their full consent, and laws have not always been reactive. Many businesses are now collecting people's personal information using seemingly harmless techniques in order to gain more money for their company by selling individuals privacy information or presenting personalised advertisements. Gathering this information is done in ways that seem safe or classified such as surveys, cookies or log on information. This information gathering goes directly against the Privacy Acts regulations of information storage. The current privacy laws for Australia are shown within the reformed Privacy Act 1988 (Cth) which constructs the process of handling an individual's information such as their name, address, telephone number, date of birth, medical records, bank account details and other classified information.

Although the Act accounts for the safe handling of information, it does not account for unauthorised access or use of this information. The case of misuse is shown through the lawsuit *Lloyd v Google LLC* [2018], presented to Google by a company named 'google you owe us'. In this case, it was presented that Google was collecting location information and many other forms of private information over a course of time and then selling it. Google faced claims that it bypassed privacy settings on Apple iPhones, collecting data on iPhone users despite the fact that the default privacy settings on those devices should have forbidden the company from tracking them. This case was dismissed by the high court as it did not cause damage to the individuals regardless of the fact, the right rights of these individuals had been violated. Therefore, it is clearly seen once more that Australian laws have not been effective in protecting an individual's rights.

Technological advancements don't just affect an individual's privacy through computers. Day to day activities can also breach individuals' rights from ineffective and invasive privacy laws. Another example where the law has failed to protect an individual's privacy is through legislation that has been introduced to give the government the power to access private communications between individuals. In December 2018, Australia's parliament introduced a new bill to bypass encrypted messaging services to inquire upon criminal activity such as terrorists, paedophiles and organised criminals said to be using these services to share information. The (Assistance and Access) Bill 2018 enhances the obligation of businesses to provide information, that would otherwise be encrypted, to be accessed by law enforcement agencies. To do this, the bill creates computer access warrants which allow police and other law enforcement agencies to access devices such as laptops, mobile phones and USBs covertly to investigate crimes, all whilst concealing from the owner that the device has been accessed. Although this legislation can come as a benefit for law enforcers to find criminals using these

---

encrypted systems, it directly breaches the rights of innocent individuals. This bill intrudes the right to privacy an individual has, as well as the right to freedom of speech and data sharing.

Although the law has attempted to stay up to date with the advancements in technology, Australian privacy laws have proved to continuously be ineffective in protecting individuals' rights in relation to privacy issues. The laws that have been put in place are brushed off by most people unless the law is implemented in a much harsher way, and there are consequences due to this behaviour. The law and penalties brought upon by wrongdoings become inexistent in people's minds resulting in these laws being unenforceable. Australia's laws on privacy have seen so little of actual stopping or protecting information from large amounts of privacy issues and continue to make irrelevant or ineffective legislature around the usage of technology and the handling of information. The ineffectiveness of Australian privacy laws in protecting an individual's rights is as a result of outdated laws still being used, a lack of understanding of different aspects for those who are creating the bills to create safe laws, private information being misused and hacked by companies and different forms of legislature being made to help the government.

edubirdie.com