Data protection

On 25 May 2018 the European General Data Protection Regulations (GDPR) (European Union, 2018) came into effect. These are the second set of regulations that have been introduced in 2018 concerning data protection. The first was the Australian Notifiable Data Breaches Act (NDBA) (Commonwealth of Australia, 2018), which was introduced on 22 February 2018, two days after the first AEGC conference ended. In response to the NDBA and GDPR, the ASEG is developing a Data Collection Policy. When the policy is finalised around August, 2018, it will be published at https://www.aseg.org.au/data-collection-policy.

The NDBA is much less proscriptive than the GDPR. Briefly, it puts the onus on organisations to decide how to proceed should they discover that data they hold has been accessed inappropriately. How organisations proceed depends on whether three criteria are satisfied:

1. there is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information, that an entity holds;
2. this is likely to result in serious harm to one or more individuals; and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

Thus, an organisation may not be required to notify affected parties in the event that they discover that data they hold has been accessed inappropriately.

The central tenet of the GDPR is that an individual’s data belong to that individual. However, it may not be clear to an individual what they own. Information that has been provided in order to access services is something that is known. Such information could be requested under the GDPR, and individuals may be notified should organisations determine they are required to do so under the NDBA.

The website https://fivethirtyeight.com recently coined the term ‘privacy of the commons’, wherein one person’s voluntary disclosure of personal information exposes the personal information of others who had no say in the matter. As shown in the recent scandal where Cambridge Analytica (The Guardian, 2018) were able to leverage information provided by users who downloaded the ‘thisisyourdigitallife’ application to profile some many (at least over 200) times more users who did not, companies can even build a profile of a person from birth based entirely on data-sharing choices made by others.

Thus, even if all searches are made using a specialised browser, all web cameras are covered, and privacy settings are monitored and updated regularly, personal data has probably still been collected, stored and used in unintended ways without an individual’s knowledge. Perhaps one small mercy is that until scandals are uncovered, ignorance is blissful.

In addition to taking the measures outlined in the previous paragraph, individuals may also test whether their email address(s) are included in known data breaches. The website https://haveibeenpwned.com/ can show hacked websites associated with an email address and indicate the nature of the breach. This knowledge can help individuals decide their next actions, such as whether to change passwords or to stop using the service. Some password managers (e.g. LastPass) can audit collected passwords to ensure strength and uniqueness.

As governments are beginning to realise, it is not clear what to do regarding an individual’s privacy now that the Pandora’s Box of connectivity and social networks has been opened. For many, the benefits far outweigh the detriments that they can monitor. The cost of an individual’s connectivity may easily be overshadowed by the profits. For many, that cost will be reduced by monitoring and maintaining security and privacy settings on all devices.

References

