Patrick Fair ASSOCIATES

UPDATE

Major Privacy Reform x2 and Security of Critical Infrastructure Bill 1

1. Discussion Paper on major Privacy Act changes

On 25 October 2021 the Federal Attorney General's Department released a Privacy Act Review - Discussion Paper. The paper proposes significant changes to the Privacy Act (**Act**) including:

- **Controls on collection:** Australian Privacy Principle 5 will be amended that reduce the amount of information that must be provided to individuals about a collection and to anticipate the creation of standard privacy notices in any Code of Practice. The Act is to include a list of factors relevant to whether or not a collection, use or disclosure of personal information is fair and reasonable. It is proposed that a party collecting personal information in a manner other than directly from the subject ensure that the original information was lawfully collected. The Act is to include a definition of the "primary purpose" of collection to mean the original collection as notified to the individual and a definition of "secondary purpose" to mean a purpose that is directly related to, and reasonably necessary to support the primary purpose.
- **Controls on use**: The Discussion paper asks for comments regarding new rules governing acts and practices considered to pose a particular risk to privacy. Referred to as "restricted and prohibited acts and practices" the list includes:
  - direct marketing,
  - collection, use or disclosure on a large scale of sensitive information from children, personal information relating to location, personal information for the purpose of influencing individual's behaviour or decisions,
  - collection, use or disclosure of biometric or genetic data including the use of facial recognition software,
  - collection, use or disclosure of personal information for the purpose of automated decision-making with legal or significant effects, and
  - any collection use or disclosure that is likely to result in a higher privacy risk or risk of harm to an individual.

  The Discussion Paper proposes two options for regulating these restricted and prohibited acts and practices:
  - the Act require parties engaging in these acts or practices to identify privacy risks and implement measures to mitigate those risks rules; or
  - changes to increase an individual's capacity to self-manage their privacy in relation to the relevant practice.

  A requirement that any use of personal information for the purpose of influencing an individual's behaviour or decisions is to be made a primary purpose notified to the individual at the time of collection.
- **New rights for data subjects:** An express right for individuals to object or withdraw consent at any time to the collection, use or disclosure of their personal information. A right to have personal information erased subject to certain exceptions. A right to object to direct marketing including an obligation to notify the individual of their right to object to each direct marketing product.

- **Compliance obligations for influencing, automated decision making, marketing and more**: A requirement that privacy policies disclose when personal information collected will be used to influence an individual's behaviour or decisions and whether or not the information will be used by third parties to provide online marketing materials and, if so, who those parties might be and how to opt out. Repeal of Australian Privacy Principle 7 (marketing). A requirement that privacy policies include information on whether any personal information will be required for automated decision-making purposes or could similarly significantly have an effect on people's rights. A proposal that pro-privacy defaults settings in any service or software be set to the most restrictive by default or have an easy way for the user to set them to the most restrictive. Australian Privacy Principle 6 to require organisations to determine each of the secondary purposes for which information is about to be disclosed and make a record accordingly. The Discussion Paper proposes a new requirement to notify data subjects of the steps aimed at mitigating harm that have been taken in response to a notifiable data breach. The information Commissioner is to obtain a new power to create industry codes of practice independently of industry and an expanded power to make emergency declarations.
- **Access and correction**: Adjustments to the rules including an obligation to advise in dividual regarding the source of any information that is being collected and a new ground of objection to supply of information requested on the basis that it relates to an external dispute resolution service and could prejudice the process. A right to consult with the subject dividual regarding any information that has been requested and provide a summary if information provided is not readily understandable
- **Changes to the rules about offshore access**: A new mechanism to prescribe countries and certification schemes and some standard clauses for the transfer of personal information offshore.

- **Overhaul of enforcement mechanism including individual rights of action**: New enforcement mechanisms, including allowing the Office of the Australian Information Commissioner (**OAIC**) to issue low level and mid-level civil penalty notices. A statutory levy of regulated organisations that are the subject of complaints in order to fund the OAIC's investigation and prosecution activities. A direct right of action for individuals or groups dissatisfied with the outcome of any complaints process. Four options for right to sue for inference with privacy:
    - a new statutory tort of invasion of privacy,
    - recognition of the existence of the tort by statute on the basis that the detail will be worked out by the courts,
    - extend the obligations under the Act to individuals in a non-business capacity so that their use collection, use or disclosure of personal information is regulated if in relation to conduct that would be highly offensive to an objective reasonable person; or
    - legislate for damages for emotional distress to be available in an action for breach of confidence.
- **More precise terminology**: A range of amendments to adjust and clarify the operation of the Act. For example, the word "about" in the definition of personal information is to be replaced with "relates to" so that any information that "relates to an identified individual will be regulated information. The term "reasonably identifiable" is to be defined and a definition of "collection" will include obtaining information by inference. References to "de-identified" is to be replaced by "anonymised". Consent will be defined as voluntary, informed, current, specific and an unambiguous indication through clear action.

Comment: These changes represent the most significant privacy reforms since the changes to the Act made in 2014. If implemented they will require revisions to Privacy Policies, Collection notices, information request handling procedures and many business practices. The changes to the penalty regime and the introduction of two forms of civil right of action, and the proposal for an industry levy to be charged to regulated entities

that are the subject of a complaint, increase the potential risk of collecting, holding and disclosing personal information. The consultation page is here. Submissions close on 10 January 2022.

2. Consultation on new Online Privacy Code power and penalties.

In conjunction with the Privacy Discussion Paper the Government released the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021. The draft legislation introduces a framework for the OAIC to make an Online Privacy Code (**Code**). Notable features of the new law include:

- The Code will regulate electronic services provided by social media services, data brokerage services, large online platforms (>2.5m users in Australia) and other organisations as may be prescribed.
- The Codes will set out "how" regulated organisations are to comply with privacy regulations including the information to be included in Privacy Policies, the provision of collection notices and obtaining consent (including for different categories of personal information).
- Regulated organisations will be required not to use or disclose personal information on request of the data subject.
- Restriction on the collection use and disclosure of personal information from children under the age of 16 and vulnerable groups including how regulated entities should handle the obtaining of parental or guardian consent.
- For social media platforms, age verification, a requirement that collection and use " be in the best interests of the child" and express consent of parents or guardians be obtained.
- Reporting obligations in relation to complaints and number of end users and enforcement obligations.

The legislation allows for the code to be developed by industry or by the Privacy Commissioner. The consultation page is here. Submissions close on 6 December 2021.

3. Security of Critical Infrastructure Bill 1 becomes law.

The Security Legislation Amendment (Critical Infrastructure) Bill 2021 was passed by both houses on 22 November 2021. Next steps underway or soon to be underway in implementing the new regulatory framework are:

- Consultation on a rule as to who the critical infrastructure register requirement and Mandatory Cyber Incident Reporting applies to.
- Consultation of the cost of implement the framework with a view to finalising the Regulatory Impact Statements for Bill 2.
- A legislative instrument to make law the modification to some of the Critical Infrastructure Asset definitions in the Act as proposed in earlier this year.
- Further work on the Risk Management Rules (recently amended to include a Governance Section).
- Tabling of Bill 2 (dealing with the Risk Management Rules and associated framework) with a view to legislating in 2021.
- After the Bill 2, the development of further sector guidelines related to the implementation of the Risk Management Rules.

For more information on the Security of Critical Infrastructure reforms, see our previous Updates.

Please contact me if you have any questions regarding the matters discussed in this update. patrick@patrickfair.com 0411361534You can subscribe to updates like this one at www.patrickfair.com