AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

Submission in response to the Privacy Act Review – Discussion Paper, December 2021

Australian Government, Attorney- General's Department

23 December 2021

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

1. ABOUT THE AUSTRALIAN DATA AND INSIGHTS ASSOCIATION (ADIA)

ADIA is the industry peak body for the market and social research industry. It has close to 100 member organisations and represents an industry that is responsible for over $1billion dollars annually in economic activity representing over 5,000 personnel.

Our members service the majority of the top 200 ASX companies and almost all state and Australian Government organisations. ADIA's key mission is the responsible and ethical collection, storage and analysis of personal and other data which can assist amongst other things, the nation's planning for future and current health programs, urban and regional planning, commuter transport, planning based on demographic trends, private and public investment, education services and much other public and private decision-making about future economic and social needs.

2. ADIA: ITS PRIVACY CODE AND ENVIRONMENT

ADIA recognises that its members have an ethical responsibility to collect, store, analyse and transmit personal data with the highest level of care and due diligence. Public trust, which includes both clients and consumers, is the critical lynchpin for our members.

ADIA therefore has taken significant steps to ensure that the community's trust is protected through several key commitments and mandatory requirements.

These include:

a) A privacy protection regime centered on a mandatory privacy code, the ADIA Privacy (Market and Social Research) Code 2021 registered under s26U of the Privacy Act 1988. This is the only industry privacy code registered under the Privacy Act and is based on the only private sector Code first registered in 2003.
b) A suite of processes to support that Privacy Code such as the continuation of an experienced Privacy Compliance Committee to provide advice, manage the Code through its Administrator (ADIA), organise and provide training and privacy awareness programs to ADIA members, survey and assist ADIA members with privacy compliance and any incidental or ongoing problems with privacy related issues and ensure that ethics and standards such as the global Market and Social Research Industry ISO 20252:2019 are complied with.
c) Regular reviews by the Privacy Compliance Committee of national and overseas developments with APEC and the OECD and International Data Protection Commissioners as well as ADIA quality assurance activities which have implications for privacy.

3. SPECIFIC RESPONSES TO THE PRIVACY ACT REVIEW AND DISCUSSION PAPER

3.1 OBJECTS OF THE ACT

Section 2A of the Privacy Act generally covers the key objectives of any national privacy regime but the *actual* coverage of the Privacy Act is limited by exclusions and the failure of the Act to include state governments, local governments and some other entities such as small business, journalism and political parties. ADIA recommends that all state government and local government entities in practice should be covered by the national Privacy Act in order to ensure that the public no longer is confused about jurisdiction when seeking information, redress or action from either the Office of the Australian Information Commissioner (OAIC) or service providers. For example, privacy protection of deceased individuals is covered in some states and not in others and where it is covered, the limits on protection also vary. There are other examples of similar variations.

ADIA understands that a national privacy regime would involve sensitive jurisdictional negotiations but if family law and defamation law can have a legal national framework, so too can privacy in an era where potentially privacy invasive technologies are increasingly sophisticated and often targeted at vulnerable minors or are capable of avoiding scrutiny from citizens confused or unaware of those privacy invasions.

To answer the question posed by the Issues Paper, 'Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, arts and practices, while ensuring clarity about protections and obligations' the answer must be no.

Since the Act was introduced in 1988 and amended significantly in 2000, a number of privacy challenging developments have occurred that will change the whole privacy protection environment. In brief these challenges are primarily:

a) the exponential growth of computing power and other technical developments,
b) Artificial Intelligence (Machine Learning),
c) sophisticated algorithms that can seek out and manipulate personal data,
d) the growth of bad actors (hackers) from state and non-state entities,
e) the widespread take-up of smart phones, other mobile devices and Internet of Things (IOT) technology,
f) the development of smart cities and COVID tracking which can have the potential to track citizens and amalgamate their personal data and,
g) the development of biometrics systems that can analyse physical and emotional attributes of a person.

3.2 DEFINITION OF PERSONAL INFORMATION

In response to the Issues question, ADIA suggests that the definition of 'personal information' could be expanded to capture technical data (such as URLs and IP addresses) and other online identifiers. ADIA notes that public opinion as surveyed by the 2020 OAIC Australian Community Attitudes to Privacy Survey (ACAP) and others is divided about the question of inferred personal information presumably on the basis that even de-identified information might possibly be amalgamated or reconstructed to create an identifiable basis of personal information. ADIA notes that its members take special care in the way they construct research in order to obviate that problem and related questions concerning technical information, de-identified, anonymous and pseudonymous information.

In conceptual terms, the European Union's General Data Protection Regulation Article 4(1) definition of personal information may provide a practical example that merits consideration, especially in relation to the privacy risks posed by metadata, AI and the capacity of machine learning to correlate technical information such as URLs and IP addresses with social media profiles. The GDPR Article 4(1) definition states that 'personal data means *any* information relating to an identifiable natural person'.

3.3 SMALL BUSINESS EXEMPTIONS

ADIA contends that all businesses, regard of size, should be brought under the ambit of the Privacy Act. ADIA's Privacy Code does not permit exemptions based on the size of the company. The Code was written on the principle that all ADIA members, regardless of size and turn-over, handle sensitive personal information to one degree or another and therefore had a duty of care to their clients, the public and their own reputations. From our experience the following reasons are advanced for all entities to be included in the Privacy Act.

a) Across many industries and government entities, outsourcing of data handling is frequent and may result in a diminution of responsibility and due diligence. There are a number of known privacy problems which can be traced back to that diminished trail of responsibility.
b) Exclusion of small enterprises from the ambit of the Privacy Act can create unfair competition from small and under-resourced entities unwilling or incapable of providing those professional services that incorporate best practice privacy policies and practices into their personal information collecting storage and use.
c) Given that some small businesses will object to the real or imagined costs of including them in the Privacy Act, ADIA still strongly recommends that all entities trading in personal information should be covered by the Privacy Act (currently, small businesses trading in personal information may be exempted from the Act provided they have the consent of individuals to collect or disclose their information). We would regard the inclusion in the

Privacy Act of all small business trading in personal information as a minimum requirement if our proposal in this section 3.3 is not accepted.

d) ADIA notes that, unlike other changes in coverage of the Privacy Act which require state and local government negotiations and co-operation, the Commonwealth Attorney-General already has the power under regulation to prescribe certain acts or business practices of small business operators to be subject to the Privacy Act.

3.4 CROSS BORDER PRIVACY RULES (CBPR)

On first appearances the adoption of CBPR in Australia seems positive given that in terms of two way trade the APEC region contains 12 of Australia's 14 partners. However, ADIA has some reservations regarding the CBPR as the current system appears to be a financial and resource imposition on businesses, with limited benefits to either clients or the businesses concerned.

3.5 THE EU'S GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR could be regarded as the most influential dedicated privacy regime in the world. For Australian businesses, the most important concern expressed by the EU authorities is the exemption for small businesses under the Australian Privacy Act.

ADIA has indicated that its own Privacy Code does include small businesses and ADIA believes all small businesses should not be exempted from the Privacy Act. ADIA accepts that, of Australia's top 15 two-way trade partners, twelve were in the APEC region and two in Europe. However, a capacity to comply with the higher privacy level of GDPR may give Australian businesses an advantage and provide a greater level of trust from consumers. This thinking is in line with ADIA's unique Privacy Code which provides a higher level of privacy compliance than the Australian Privacy Act itself. (See 3.6, the ADIA Privacy Code).

3.6 ADIA's INDUSTRY PRIVACY CODE

ADIA takes its privacy obligations extremely seriously. The organisation recognizes that its members deal with personal information as their main business; therefore, the highest level of privacy compliance is a keystone of what our members do daily and in terms of long-term strategies for the industry.

Public trust is essential to ensure that Australians are willing to provide their personal information in the interest of the societal improvements that come from the collection, analysis and use of that information, whether that personal information be longitudinal health studies or demographic planning data to enable Governments and businesses to invest in services or assets that this country requires.

a) ADIA members recognize that our Privacy Code that has compliance and coverage levels higher than the Australian Privacy Act provides significant

value and, although this requires more due diligence and resourcing, that investment is beneficial for clients, ADIA members and the public at large.

b) ADIA also recognized that compliance with privacy requirements is often not automatic but requires consistent progress and improvements from each member of ADIA. As a result, ADIA's strategy to ensure that qualitative privacy improvement has taken several fronts. These are, the establishment and resourcing of a Privacy Compliance Committee, the reporting to and continuing liaison with the OAIC, the provision of privacy training for ADIA members, a privacy trust mark system, follow-up work to ensure that all members are compliant, and a system of sanctions and assistance should the level of compliance not be satisfactory.

3.7 EMPLOYEE RECORDS EXEMPTION

ADIA holds the view that some further protection for employee records should be included in the Privacy Act since:

a) Those records are likely to contain significant personal information.
b) The inappropriate release of that personal information could have disadvantageous consequences for the employee.
c) Issues such as DNA and other biometric collection and retention now makes employee records that much more sensitive as those records often contain some health information that could be significantly out of the control of the individual. Many ADIA members operate in the health research area, especially with longitudinal studies and they are acutely aware of the security, ethics and best practice required in that type of research.

However, ADIA shares the concern of other business groups that care needs to be taken in the design of any legislative amendment in this area to ensure that employers retain flexibility to effectively and efficiently manage their employment relationships. Accordingly, ADIA submits that the existing exemption should be modified to allow better protection of employee records while retaining the flexibility employers need to administer the employment relationship.

3.8 POLITICAL PARTIES EXEMPTION

Political parties' exemption from the Privacy Act is not acceptable given that political parties and the entities and individuals that work for them collect significant amounts of personal data and recently have shown that they use this data to make highly targeted unsolicited calls and texts to the public. Politicians also have a protected free speech forum under Parliamentary privilege.

3.9 JOURNALISM EXEMPTION

ADIA accepts that journalists should continue to be exempted from provisions of the Privacy Act provided that they work within the framework of legislation such as defamation law and appropriate national security laws. The right to free

speech is a fundamental right in a democratic society and it is accepted that, from time to time, personal information may enter the public sphere despite the objections of the subjects, especially public figures. The interests of society rely on a free press and transparency in public and corporate life.

3.10 NOTICE OF COLLECTION OF PERSONAL INFORMATION AND OTHER PRIVACY ISSUES

In terms of improving the standard of privacy policies and practice, ADIA sees great value in certain industries subjecting themselves to the rigour and best practice framework of specific industry codes. This allows a codified framework to be established which has the effect of law and can work well, especially in industries which collect and transact personal information.

ADIA's Privacy (Market and Social Research) Code 2021 covers most matters raised under this issue. ADIA members recognize that industry longevity relies on the trust and co-operation of the public and those they interact with. Our Privacy Code has been designed to ensure that awareness, understanding, and consent are an essential part of what the public expects from our members. Industry codes can be specific, targeted and easier for members to understand and act on information issues most relevant to our members, their clients and the public with whom they engage.

ADIA is therefore concerned that many online 'researchers' or service providers that are not ADIA members and not signatories to our mandatory Privacy Code will continue to use online questionnaires that contain few privacy protections. Those protections relate especially to consent and other areas where the consumer is asked sensitive questions without the service provider being required to provide details and gain informed consumer consent about the purpose, use and ultimate destination of their personal information.

This is why ADIA members are willing to maintain quality and trust by signing up to the requirements of the ADIA Privacy Code. Some of the key requirements covered by our Code and associated practices include:

a) Ease of access for the public to find more information about their rights especially the opportunity to make complaints and seek redress.
b) A Privacy Compliance Committee which includes an independent chair, an industry representative, a consumer representative, a legal representative, and a secretary. This committee meets twice a year and regularly communicates on key issues as well as taking part in training and awareness sessions for ADIA members.
c) Training in privacy related issues is online-on demand, provided through regular privacy updates and special sessions. A portal is provided for training in best practices through the ADIA Academy. A list of the training modules and the Compliance Updates provided to members is attached at Appendix A.

d) A Privacy Compliance Checklist which is administered by the ADIA Administrator who then is required by law to report to the Office of the Australian Information Commissioner. The report must include the names of organisations which have completed the check list. Completion of the checklist will be mandatory in 2022.
e) The check list also helps members to identify gaps in their expertise or processes they follow.
f) ADIA's Privacy Compliance Committee needs to report any serious and repeated privacy breaches and any systemic issues about Code compliance. All breaches are reported including basic issues such as the non-appointment of a privacy officer through to more serious breaches such as failure to respond to or an incapacity to respond to complaints or enquiries or loss or misuse of personal information.
g) A requirement for ADIA members to keep accurate records which will allow them to report to ADIA.
h) Provisions in the Code to guide ADIA members in specific research and marketing procedures related to personal information. These procedures include requirements relating to Access Panels, disclosure of personal information, device monitoring, cookies, opt-out procedures for panels etc.
i) ADIA maintains a list of the privacy officers from all member companies and follows up those that fail to appoint a privacy officer.
j) The operations and content of the ADIA Privacy (Market and Social Research) Code 2021 are reviewed by an independent auditor and the recommendations adopted by the ADIA Privacy Compliance Committee. The Code Administrator also is required to conduct an annual review of ADIA members' privacy compliance. Under its privacy code ADIA is also required to report comprehensively to the OAIC. The OAIC then can require changes to the Code or look at ADIA member practices.

3.11 STATUTORY TORT

ADIA is generally in favour of a statutory tort for invasion of privacy being introduced in Australia. If the alternative is a more complex, prescriptive and highly regulated privacy regime with all its compliance and potential hazards, ADIA sees the statutory provision of tort rights as a superior alternative. Legislation is not always able to keep up with technology change and market driven innovation; hence ADIA's preference for a statutory tort that constitutionally would become an established right, allowing individual action to add to the legislated and practice responsibilities of the OAIC commissioner.

ADIA is satisfied with a system where the OAIC Commissioner is the first port of call for complaints about privacy breaches since conciliation and a filter for vexatious complaints needs to exist before any tort action against egregious breaches of privacy can commence.

3.12 NOTIFIABLE DATA BREACHES SCHEME (NDB)

ADIA has been highly active in training and monitoring its members in matters related to notifiable data breaches. Our feedback to the OAIC is that the NDB scheme has worked to heighten member awareness and prompt them to establish procedures and preparations for NDB best practice.

3.13 INTERACTION BETWEEN THE ACT AND OTHER REGULATORY SCHEMES

ADIA does recognize that there are many overlapping regulations and law in the processing and management of personal information. Our members are required to deal across a number of other regulatory environments such as our Code, health information management, ethics requirements and state laws.

There would appear to be a benefit for some amalgamation as in defamation law, but ADIA believes that such a process would require long term planning and co-operation between many entities that govern the privacy space. In the meantime, ADIA is satisfied that an industry code such as the ADIA Privacy (Market and Social Research) Code 2021 and the relevant ISO standards such as ISO 20252:2019 provides a satisfactory framework for our members and generally can be useful in our members in their dealings with other international jurisdictional law such as GDPR.

3.14 CONTROL AND SECURTY OF PERSONAL INFORMATION

ADIA's members often conduct long term longitudinal studies in areas such as health, urban planning, economy and finance. Those long-term studies necessitate the retention of personal data (usually de-identified or anonymised) for benchmarking and other research-based purposes.

The ACCC proposed that the right to erasure should not override contractual obligations, legal factors, industry specific laws, tax requirements, healthcare purposes and law enforcement requirements. The European Union's GDPR is the strongest privacy protection regime in the world but, on the question of the right to be forgotten (erasure) its Article 17 also exempts activities such as journalism, academic work, artistic or literary expression, statistical work, scientific or historical research and provides exemptions for commercial entities in some circumstances.

ADIA's critical role in assisting research and future planning obviously persuades us to recommend that the right to erasure should continue to be mitigated for the above reasons.

APPPENDIX A: ADIA's WEBINARS and PRIVACY and DATA SECURITY-COMPLIANCE UPDATES and the ADIA ACADEMY.

The following ongoing support and guidance has been provided to ADIA members over the last year primarily through the ADIA Academy's on-demand training portal:

1. Risk Management-Privacy and Quality Assurance Webinars
   a) Transitioning to ISO 20252:2019
   b) Internal Auditor Training ISO 20252:2019
   c) DIY Information and Data Security Compliance
   d) Document and Data Control
   e) Privacy Information Security ISO 20252 Synergies
   f) The New Privacy Code (2021)

2. Privacy and Data Security-Compliance Updates
   a) Data Protection Laws of Australia
   b) Assistance and Access Laws of Australia
   c) Consumer Rights Laws and Data and Insights research Industry
   d) The Right to be Forgotten-Erasure
   e) New Zealand Privacy Laws
   f) Anonymity and Pseudonymity
   g) Cyber Security for Mobile Devices
   h) QR Codes
   i) Policies, Policies and More Policies.

For further information:

The Hon. Terry Aulich
Chair
ADIA Privacy Compliance Committee
E: aulichterry8@gmail.com

Sarah Campbell
CEO
ADIA
E: Sarah@dataandinsights.com.au