THE AUSTRALIAN DATA AND INSIGHTS ASSOCIATION (ADIA)

SUBMISSION TO THE PRIVACY ACT REVIEW

AUSTRALIAN FEDERAL GOVERNMENT ATTORNEY GENERAL OFFICE

MARCH 2023

INTRODUCTION

ABOUT THE AUSTRALIAN DATA AND INSIGHTS ASSOCIATION (ADIA)

ADIA is the industry peak body for the Australian market and social research industry. It has close to 100 member organizations and represents an industry responsible for over $ 3 billion annually in economic activity representing over 5000 personnel.

THE VALUE OF EVIDENCE-BASED RESEARCH

ADIA 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.

Sound government policy and commercial business decisions depend on trusted, high-quality, evidence-based research.

ADIA: ITS PRIVACY CODE AND ENVIRONMENT

ADIA recognizes that its members have a legal and ethical responsibility to collect, store, analyze and transmit personal data with the highest level of care and due diligence. Public trust, which includes clients, research respondents and consumers, is the critical lynchpin for our members.

Market and social research conducted by ADIA member organisations is collected only with specific and informed consent and under strict codes and practices. ADIA and its members take 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, ADIA's Privacy (Market and Social Research) Code 2021 registered under s26U of the Privacy Act 1988 by the Australian Information Commissioner, Angelene Falk, March 1, 2021. It remains the first 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 (via the ADIA Academy), 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.

SPECIFIC RESPONSES TO THE PRIVACY ACT REVIEW

ADIA welcomes the opportunity to participate in the Privacy Act Review and believes the proposed changes are timely and relevant. We support the view that all Australian entities have a responsibility to ensure that their information handling practices are fair and not harmful and have advocated for some time the need to beef up consumer privacy protections by increasing consent and notification requirements like those undertaken by ADIA members working under the industry Privacy Code. Given the ever-increasing uptake of data-driven services and level of technological innovation, the proposed enhanced protections bear even greater importance and meaning.

PROPOSAL 3. OBJECTS OF THE ACT

ADIA supports amendments to the Act to clarify that the Act is about the protection of personal information.

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 does not include state governments, local governments, and some other entities such as small business, journalism and political parties.

ADIA agrees 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 has greater clarity about the appropriate jurisdiction when seeking information, redress or action from either the Office of the Australian Information Commissioner (OAIC) or service providers.

ADIA understands that a national privacy regime would involve sensitive jurisdictional negotiations but if workplace relations, 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.

PROPOSAL 4. THE DEFINITION OF PERSONAL INFORMATION

ADIA supports that the definition of 'personal information' be amended to ensure greater clarity and transparency overall in regard to the connection between information and the individual is not tenuous or remote.

Proposal 4.3 - In principal, ADIA also agrees with the expansion of the definition of collection (to capture technical data and other online identifiers) however notes that while ADIA 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, ADIA looks forward to receiving the list of circumstances members are expected to have regard in their assessment.

Proposal 4.5 & 4.6 – Amending the definition of de-identified. Market and social research best practice requires researchers to de-identify survey results as soon as possible. Anonymity remains a top priority as research is not interested in the name of a survey respondent, but their opinion.

PROPOSAL 6. SMALL BUSINESS EXEMPTION

All ADIA member organisations, regardless of annual turnover, work under the Privacy Code. The Code was written on the principle that all ADIA members, (regardless of size and turnover), handle sensitive personal information to one degree or another and therefore have a duty of care to their clients, the public and their own reputations.

ADIA therefore supports the recommendation that all businesses should be brought under the scope of the Privacy Act (subject to the impact analysis). 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 protection issues 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 being covered by the Privacy Act, ADIA strongly recommends that all entities *trading in personal information* should be covered by the Privacy Act.
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.

PROPOSAL 7: EMPLOYEE RECORDS EXEMPTION

ADIA supports the proposed amendment to enhance privacy protection and transparency for individuals working in the private sector. Ensuring an employee's personal information is collected with consent, protected from misuse, and stored safely and appropriately, minuses risk and will benefit both employer and employee.

a) Those records are likely to contain significant personal information, including sensitive information.
b) The inappropriate release of that personal information could have significant negative 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.

PROPOSAL 8. POLITICAL PARTIES EXEMPTION

ADIA supports this amendment and the recommendation 8.4 (a)(b) which provides an individual with the ability to opt-out'. The political parties' exemption from the Privacy Act is not desirable 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.

PROPOSAL 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 other relevant legislation, such as defamation law and appropriate national security laws. The right to free speech is an implied constitutional right 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.

ADIA agrees with the proposal to conduct an independent review (9.3) of the journalist exemption every three years. Furthermore, that media organisations comply with security and destruction obligations as per APP 11. Ensuring that personal information is protected from misuse, interference is every organisations responsibility.

PROPOSAL 10. PRIVACY POLICIES AND COLLECTION NOTICES
PROPOSAL 11. CONSENT AND PRIVACY DEFAULT SETTINGS

We support introducing an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable.

As part of ADIA's administrator duties with the Privacy (Market and Social Research) Code 2021, the Association provides members templates and guidance to ensure our members are fully aware of their obligations working under APP5.

Furthermore, ADIA sees great value in certain industries subjecting themselves to the rigor 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 proposal. ADIA members especially require 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. The proposal to amend the definition of consent to provide that it must be voluntary, informed, current specific and unambiguous brings it in-line with the industry privacy code and code of ethics – as research is always conducted with informed and explicit consent.

As indicated in our previous submission, ADIA supports this amendment and acknowledges that it would change the current practices of online 'researchers' or service providers that are not ADIA members and not signatories to our mandatory Privacy Code. The protections outlined in proposal 11 relate specially 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 member organisations (large and small) 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 are:

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) An annual Privacy Compliance questionnaire 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.
e) The questionnaire 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 privacy officers from all member companies and follows up those that fail to appoint a privacy officer.

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 is also 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.

PROPOSAL 13. ADDITIONAL PROTECTIONS

In principle, ADIA supports the amendment that PIAs be conducted for activities with a *high privacy risk* however we would also submit that, for ADIA members, working under a privacy code – which sets out a clear, industry specific APP roadmap – this could result in additional work for limited public benefit.

PROPOSAL 16. CHILDREN

ADIA members working under the privacy code and the industry code of conduct must adhere to strict professional standards and practices when working with children.

Researchers must take special care when interviewing children and young people. The consent of a parent or responsible adult must first be obtained before collecting information from:
a) children, defined as under 14 years, and
b) young people, defined as 14-17 years, when sensitive information is being collected.

Sufficient details about the project should also be given to the parent or responsible adult to enable them to give informed consent. This includes:

- the name and contact details of the organisation conducting the research
- the type of information that will be collected
- the reasons for selecting the child and any impacts the interview may have on the child
- a description of the procedure for giving consent
- an explanation of how the child's identifiable research information will be used and protected and
- an explanation of any product testing.

Given the industry's long-standing commitment to privacy protection when working with children, ADIA would welcome the opportunity to work with the OAIC or the ACMA to support the development of the proposed *Children's Online Privacy Code*.

PROPOSAL 18. RIGHTS OF THE INDIVIDUAL

In principle, ADIA supports the proposal and the *right to be forgotten*, subject to the nature of the collection. In some cases, however, it is not reasonably practicable for respondents to be forgotten and note APP 10 and the Privacy Code explanatory material as follows:

In the research context, research data is recorded at a point in time (e.g. the interview or completion of a questionnaire), and it would not be appropriate to change or update the data, even if the respondent later felt that the data did not represent their current views – see below re correction rights.

If a Research Organisation retains identifiable research information, when using or disclosing that information, it should:

a) where it concerns research data, warrant that the information is an accurate and complete record of the information supplied at the time of collection; and
b) where it concerns identifiable research information other than research data (i.e., contact details or research status), take reasonable steps to ensure that the information remains accurate, up to date, complete and relevant.

We also note APP 13 and the following explanatory note as included in the Privacy Code:

Explanatory Note:
If a Research Organisation receives a request from an individual to correct his or her identifiable research information, the Research Organisation's response should depend on the type of information:
Where the request concerns research data, the Research Organisation should:
i. explain to the individual that it may not be possible to correct research data where it must remain an accurate and complete record of the information at the time of collection; but also
ii. at the request of the individual, associate with the information a statement that the information is (in the individual's opinion) inaccurate, out of date, incomplete, irrelevant or misleading.

Because of the importance of maintaining the integrity of research, Research Organisations will generally decline to correct research data (survey responses), offering only the option of an associated statement where practicable, and information about the right to complain to the OAIC or recognised External Dispute Resolution (EDR) scheme where applicable. (No such EDR schemes are available at the commencement of this Code.) In limited cases, it will be impracticable to associate a statement because of the way the research data is held.

Where the request concerns identifiable research information other than research data (i.e., contact details or research status), the Research Organisation should either:

i. correct the information so that it is accurate, up to date, complete, relevant and not misleading; or
ii. where a record of the uncorrected information is required for research purposes, associate with the information a statement that the information is (in the individual's opinion) inaccurate, out of date, incomplete, irrelevant or misleading.

PROPOSAL 21. SECURITY, RETENTION AND DESTRUCTION

ADIA members working under the Privacy Code adhere to the following additional requirements to ensure that all personal information collected for the purpose of research is secure and disposed of in a safe and timely manner.

The Privacy (Market and Social Research) Code 2021 reads:

Additional Requirement: retention and disposal

11.3 A Research Organisation must retain identifiable research information only while the details of the identity of the individual whom the information is about continue to be necessary to be retained for research purposes. The information must be destroyed or de-identified once these purposes have been achieved. Where identifiable research information has been returned to a third party (in accordance with APP 6), any copies, including archived copies, must be destroyed or de-identified.

If a Research Organisation wishes to de-identify identifiable research information that exists in a physical form that makes de-identification impracticable (e.g. on paper), the information must be moved to another medium, de-identified, and the physical records then destroyed.

Where it is necessary to retain identifiable research information, identifying (contact) details must, if practicable, be stored separately from other information (research status and research data), with measures in place (e.g. by the use of an encrypted intervening variable) to ensure the identity of the individuals cannot be readily revealed from the other information.

A Research Organisation must take reasonable steps to ensure that any identifiable research information that it discloses:

a. will be retained, used or disclosed by the recipient of the information only in a manner that is consistent with this Code; and

b. will be protected by the recipient from misuse, interference and loss and from unauthorised access, modification, use and disclosure; and

c. will be used or disclosed by the recipient only for a specified limited purpose and will be destroyed or de-identified once this purpose has been achieved. Where identifiable research information has been returned by the recipient to a third party (in accordance with APP 6) any copies, including archived copies, must be destroyed or de-identified.

A Research Organisation may disclose de-identified information freely, provided that there is no reasonable likelihood that the disclosed information could be used to identify one or more of the individuals who participated in the research, such as where the pattern of answers could reveal their identity.

Additionally, a majority of our members are certified to the ISO 20252:2019, and in some cases also certify to ISO 27001 (Information Management Security Standard).

ADIA is therefore not opposed to these amendments. Our members would however benefit from further consultation and information from the OAIC regarding changes to their guidelines and technical advice/support from the Australian Cyber Security Centre (ACSC).

PROPOSAL 27: STATUTORY TORT FOR SERIOUS INVASION OF PRIVACY

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.

PROPOSAL 28. 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.

ADIA supports the amendment but with a 7-day notification period.

PROPOSAL 29. INTERACTION BETWEEN THE ACT AND OTHER REGULATORY SCHEMES

ADIA acknowledges that there are many overlapping regulations and laws in the processing and managing of personal information. Our members must deal with several regulatory environments, such as our Code, health information management, ethics requirements and state laws. With that in mind, there would be a benefit for some amalgamation, as is the case with defamation law. ADIA supports establishing a Commonwealth, state and territory working group that harmonizes privacy law and, importantly, keeps abreast of key issues and changes in this age of technology.

ADIA welcomes the opportunity to further engage with the Attorney General's Office, the Office of the Australian Information Commissioner, and other stakeholders on the proposed privacy reforms.

For further information: Sarah Campbell CEO ADIA sarah@dataandinsights.com.au

APPPENDIX: ADIA's PRIVACY and DATA SECURITY-COMPLIANCE TRAINING via THE ADIA ACADEMY.

ADIA offers specialist privacy law advice for members via Andrew Maher (ADIA's legal counsel via the member hotline) and Sarah Campbell CEO, ADIA, and ADIA Privacy Compliance Committee members.

To further support our member's compliance to the Privacy (Market and Social Research) Code 2021, ADIA continues to offer a suite of training and guidance materials on best privacy practices via the ADIA Academy, an on-demand online training portal.

The ADIA Academy platform offers members the following specialised privacy modules:

- Induction 101 (Privacy & APP)
- Advanced Induction 1 – Privacy and Data Security
- Advanced Induction 2 – Risk Management and PIA

There is also a range of information security and auditing training modules on the platform for members to undertake at their convenience https://dataandinsights.com.au/member-benefits/training