PMSR Code Review 2019

Review report of the Independent Reviewer appointed by the Association of Market and Social Research Organisations to conduct a review of the Privacy (Market and Social Research) Code 2014

Peter G Leonard

March 2020

PMSR Code Review 2019

This document is a review report prepared by the Independent Reviewer[1] appointed by the Association of Market and Social Research Organisations ABN 20 107 667 398 (**AMSRO**) to conduct a review of the Privacy (Market and Social Research) Code 2014[2] (the **PMSR Code**), as registered under s 26U(1) of the Privacy Act 1988 (**Privacy Act**) on 28 November 2014.[3]

This review is commissioned by AMSRO to fulfil requirements of the PMSR Code and of the Privacy Act as to periodic review of a registered code. These requirements are summarised later in this review report.

By way of full disclosure, this review has been commissioned and paid for by AMSRO.

However, this review states the views of the Independent Reviewer, not AMSRO.

A corresponding review was conducted in February 2013 by Dr Terry Beed, Director of the Centre for Survey Quality Assurance. The focus of that review by Dr Beed was a predecessor code to the PMSR Code, The Market and Social Research Privacy Code 2012. Dr Beed's 2013 findings informed development and drafting of the PMSR Code.

This document summarises the first independent review of the current PMSR Code.[4]

Scope of this Review

This review of the PMSR Code has included evaluation and consideration by the Independent Reviewer of:

- the current state of good data privacy risk management practices as relevant to conduct of each stage of conduct of market, opinion and social research and reporting as to outputs of that research, including measures to ensure the reliability

[1] Peter Leonard is a data, content and technology business consultant and lawyer advising data-driven business and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (IT Systems and Management, and Business and Taxation Law). Peter chairs the IoTAA's Data Access, Use and Privacy work stream, the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of corporate and advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. The views expressed in this review report are those of the author not those of any of those other bodies and organisations.

[2] Available at https://www.legislation.gov.au/Details/F2014L01725.

[3] https://www.legislation.gov.au/Details/F2014L01725/Supporting%20Material/Text

[4] Dr Terry Beed, Director of the Centre for Survey Quality Assurance, Strategic Review of The Market and Social Research Privacy Code 2012: An Independent Code Review.

of pseudonymisation and deidentification techniques and methods that are used to protect personal information about participating individuals,

- whether the PMSR Code gives sufficient guidance and incentive for research organisations to adopt good data privacy risk management practices and comply with other requirements of the PMSR Code and the Privacy Act,
- whether the PMSR Code provides sufficient transparency as to detection of, and actions to address, poor or unacceptable data practices or other non-compliances by research organisations with requirements of the PMSR Code and the Privacy Act, such that the OAIC and the general public should have confidence that the PMSR Code will be given practical effect.

This review also included consideration of:

- The extent of knowledge of the general public as to the existence and operation of the PMSR Code.
- Whether the operation of the Code should be limited to AMSRO members.
- How the current (2014 version) of the PMSR Code could be improved in scope and clarity.
- What had changed since 2014 which needed to be now covered.
- What content could be removed or simplified because that content was better covered in another readily available resource (such as the Office of the Australian Information Commissioner (**OAIC**) Australian Privacy Principles guidelines).[5]
- Developing international best practice in relation to development of codes of conduct and industry codes of practice, and in particular the European Data Protection Board Guideline 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.[6]
- Developing international best practice in relation to conduct of market, opinion and social research and data analytics.

AMSRO and its role in the PMSR Code

The PMSR Code was developed and is managed by AMSRO.

AMSRO is the peak organisation of Australian market and social research organisations. AMSRO's focus is activities of research organisations in relation to their conduct of market, opinion and social research for clients of the respective research organisations.

AMSRO is an 'APP code developer', as defined in s 6(1) of the Privacy Act, of the PMSR Code.

[5] As available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
[6] Version 2.0, 4 June 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

The PMSR Code is published by AMSRO on the AMSRO website[7], as well as being available through the OAIC website[8] and the Federal Register of Legislation[9].

The PMSR Code is binding on AMSRO members, referred to as 'research organisations' in the PMSR Code. AMSRO has approximately 90 members[10]. These research organisations are estimated by AMSRO to collectively employ over 5,000 people and represent about 70% of the research organisation sector's annual turnover.

AMSRO states AMSRO's aims as follows:

- represent and enhance the research[11], data analytics[12] and insights[13] industry,
- advise, represent and advocate on behalf of AMSRO members,
- encourage confidence and minimise risk in client decision making by clients of research organisations, and
- to ensure industry standards are relevant, appropriately promoted and recognised.

AMSRO states that it seeks to achieve these objectives by:

- working to improve awareness and regard for market and social research organisations,
- working to improve the quality and professionalism of market and social research practices,
- representing the interests of members to government, regulators and other stakeholders,
- helping develop and retain talent in the industry,
- providing members with workplace relations advice and support, and
- promoting the exchange of information among industry leaders.

In its capacity building role, AMSRO conducts workshops and seminars for research organisations and other interested parties, and publishes a range of guidance and training materials for research organisations, including:

[7] The website is at ; the Code is available at https://www.amsro.com.au/member-services/privacy/
[8] https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/market-and-social-research-code/
[9] https://www.legislation.gov.au/Details/F2014L01725
[10] A list is available at https://www.amsro.com.au/list-of-members/.
[11] Research includes all forms of market, opinion and social research and data analytics, is the systematic gathering and interpretation of information about individuals and organisations. It uses the statistical and analytical methods and techniques of the applied social, behavioural and data sciences to generate insights and support decision-making by providers of goods and services, governments, non-profit organisations and the general public.
[12] Data analytics is the process of interrogating data to identify patterns, correlations, trends or other information. This also includes modelling, forecasting and aggregation of data.
[13] Insight is the value obtained through the use of analytics, often expressed in the form of a deduction (e. g. women aged between 25 and 34 in Australia are more much likely to buy iPhones (as against Android devices) than men in the same age cohort).

- Industry training modules[14]
- Quality Assurance and Risk Management guidance materials and tools,[15] including as to compliance with and accreditation to ISO 20252:2019 Market, opinion and social research;[16]
- Guide to the Notifiable Data Breaches (NDB) scheme
- Privacy Awareness and Compliance Information and Tools
- Guidance as to application of the ICC/ESOMAR Code[17]
- Webinar presentations
- Guide to Reporting requirements under the industry privacy code
- The role of the Privacy Compliance Committee and making a complaint

The AMSRO Privacy Compliance Committee meets twice a year to examine privacy matters relating to the PMSR Code and provides regular updates and training to members and the AMSRO Board on privacy related matters.

The members of this Committee for the 2019 reporting year were:

Terry Aulich	Independent Chair
David Vaile	Consumer representative
Szymon Duniec	Industry representative
Andrew Maher	Legal representative

[14] Available through https://www.amsro.com.au/member-services/privacy/privacy-law-industry-training-modules/

[15] Available through https://www.amsro.com.au/member-services/quality-assurance/

[16] Available at https://infostore.saiglobal.com/en-au/Standards/ISO-20252-2019-589547_SAIG_ISO_ISO_2705481/

[17] ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics, available at https://www.esomar.org/what-we-do/code-guidelines. See also ESOMAR Guideline on Social Media Research, available at https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-Guideline-on-Social-Media-Research.pdf; ESOMAR/GRBN Online Research Guideline, available at https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-GRBN-Online-Research-Guideline-October-2015.pdf; ESOMAR/GRBN, Guideline on Mobile Research, available at https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-GRBN-Guideline-on-Mobile-Research.pdf; ESOMAR/GRBN, Guideline on Research and Data Analytics with Children, Young People, and Other Vulnerable Individuals, available at https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-GRBN_Guideline-on-Research-and-Data-Analytics-with-Children-Young-People-and-Other-Vulnerable-Individuals_2018.pdf; draft for consultation (as at February 2020) ESOMAR/GRBN Guideline for Researchers and Client Involved in Primary Data Collection, available at https://www.esomar.org/what-we-do/code-guidelines/primary-data-collection-guideline; draft for consultation (as at February 2020) ESOMAR/GRBN Guideline on Duty of Care: Protecting Data Subject from Harm, available at https://www.esomar.org/what-we-do/code-guidelines/duty-of-care-guideline. For a useful review of ethical and data privacy issues involved in market and social research, see Reg Baker and Norbert Wirth, Discussion Paper: Use of Secondary Data in Market, Opinion, and Social Research and Data Analytics, February 2018, and sources there cited, available at https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-GRBN_discussion-paper_Use-of-Secondary-Data_20180225.pdf.

Sarah Campbell Secretary (Executive Director, AMSRO)

The Committee publishes an annual report summarises its relevant activities, including its oversight of the Code.[18]

AMSRO also operates a successful "Privacy Quality Ethics" Trust Mark scheme.[19] The Trust Mark is an indicium that qualifying AMSRO member organisations:

- have been audited and certified as to compliance with ISO 20252:2019 Market, opinion and social research, and
- adhere to the AMSRS Code of Professional Behaviour (see below), and
- adhere to the PMSR Code.

All AMSRO members must comply with the PMSR Code as a condition of membership of AMSRO. By contrast, only those AMSRO members that have also met the additional criteria (that is, audited and certified to ISO 20252:2019, and a commitment that research professionals engaged by the AMSRO member will adhere to the AMSRS Code of Professional Behaviour) are authorised to display the AMSRO Trust Mark.

The Independent Reviewer's review of the websites and online published privacy policies of a random selection of members found that almost all AMSRO members in the group referenced the PMSR Code and all AMSRO members in the group that were authorised to display the AMSRO Trust Mark did so.

AMSRS and the role of AMSRS

A separate organisation, the Australian Market & Social Research Society Limited (**AMSRS**), represents market and social research individual professionals and is "dedicated to increasing the standard and understanding of market and social research in Australia".[20]

AMSRS states that it has over 2,000 market and social research individual members and 80 Company and Client Members.

A condition of membership of AMSRS is adherence to the AMSRS Code of Professional Behaviour (the **AMSRS Code**), which is designed as a framework for self-regulation by AMSRS members.

The stated objectives of the AMSRS Code are:

- to set out the ethical rules which market and social researchers must follow;
- to enhance the public's confidence in market and social research by emphasising the rights and safeguards to which they are entitled under the Code; and

[18] https://www.amsro.com.au/member-services/privacy/amsro-privacy-compliance-committee/
[19] https://www.amsro.com.au/member-services/trust-mark/
[20] https://www.amsrs.com.au/

- to minimise the need for governmental and/or intergovernmental legislation or regulation.[21]

The AMSRS Code covers many aspects of ethical and fair behaviour of market and social research professionals when conducting research, including (but ranging significantly beyond) compliance with privacy laws and meeting reasonable expectations of privacy of individuals participating in research (that is, the data subjects of the research).

A formal complaints procedure exists for breaches of the AMSRS Code.

AMSRS members are required to adhere to the AMSRS Code. [22]

AMSRS also publish useful resources for the general public about market and social research.[23]

The Market Research Society, a United Kingdom organisation with a corresponding role and functions to the AMSRS, revised its Code in October 2019.[24] That revised Code provides a useful point of comparison to the AMSRS Code.

ISO 20252:2019 Market, opinion and social research[25]

This international and Australian standard was substantially rewritten in 2019 and combines two predecessor ISO standards – 20252 & 26362.

The standard covers the planning, execution and reporting stages of research, including research proposals, designing questionnaires and discussion guides, sampling and data processing, archiving documents, and conduct of quantitative and qualitative research, including self-completion and observational data collection, both online and offline.

Good data management and processing practice is defined through provisions in the standard as to coding, analysis, document retention and data security and data privacy, including human resource considerations such as recruitment and training of fieldworkers.

Research organisations certified under the predecessor standards have until December 2020 to achieve certification to this new standard.

[21] https://www.amsrs.com.au/professional-standards/code-of-professional-behaviour
[22] As to enforceability of the AMSRS Code, see also the AMSRS Regulations available at https://www.amsrs.com.au/documents/item/786
[23] See https://www.amsrs.com.au/about/information-for-the-general-public.
[24] Market Research Society, Code of Conduct - October 2019 available at https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf.
[25] Market, opinion and social research, including insights and data analytics -- Vocabulary and service requirements, available at https://infostore.saiglobal.com/en-au/standards/iso-20252-2019-589547_saig_iso_iso_2705481/

ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics[26]

This Code (the **ICC/ESOMAR International Code**) has a similarly broad focus to the AMSRS Code of Professional Behaviour.

The ICC/ESOMAR International Code also references provisions[27] of the ICC Code of Marketing and Marketing Communications Practice (Version 2.0, 4 June 2019) which addresses marketing related communications more generally, while the ICC/ESOMAR International Code focuses only upon the market, opinion and social research sector.

The ICC/ESOMAR International Code is stated to be:

> "based upon three fundamental principles that have characterised market, opinion and social research throughout its history. They provide an interpretative background for the application of the substantive articles of the Code:
>
> 1. When collecting personal data from data subjects for the purpose of research, researchers must be transparent about the information they plan to collect, the purpose for which it will be collected, with whom it might be shared and in what form.
>
> 2. Researchers must ensure that personal data used in research is thoroughly protected from unauthorised access and not disclosed without the consent of the data subject.
>
> 3. Researchers must always behave ethically and not do anything that might harm a data subject or damage the reputation of market, opinion and social research."

Articles 1 to 6 of the ICC/ESOMAR International Code address "Responsibilities to data subjects" as follows:

Article 1 Duty of care

(a) Researchers must ensure that data subjects are not harmed as a direct result of their personal data being used for research.
(b) Researchers must exercise special care when the nature of the research is sensitive or the circumstances under which the data was collected might cause a data subject to become upset or disturbed.
(c) Researchers must remain mindful that research relies on public confidence in the integrity of research and the confidential treatment of the information provided for

[26] https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ICCESOMAR_Code_English_.pdf. See also the ESOMAR Data Protection Checklist, June 2017, at https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-Data-Protection-Checklist_September-2017.pdf

[27] In particular, Article 9 of the consolidated ICC Code of Marketing and Marketing Communications Practice, which states: "Marketing communications should not misrepresent their true commercial purpose. Hence a communication promoting the sale of a product should not be disguised as for example market research, consumer surveys, user-generated content, private blogs or independent reviews".

its success, and therefore must remain diligent in maintaining the distinction between research and non-research activities.

(d) If researchers engage in non-research activities, for example promotional or commercial activities directed at individual data subjects, they must clearly distinguish and separate those activities from research.

Article 2 Children, young people and other vulnerable individuals

(a) Researchers must obtain the consent of the parent or responsible adult when collecting personal data from children or anyone for whom a legal guardian has been appointed.

(b) Researchers must take special care when considering whether to involve children and young people in research. The questions asked must take into account their age and level of maturity.

(c) When working with other vulnerable individuals, researchers must ensure that such individuals are capable of making informed decisions and are not unduly pressured to cooperate with a research request.

Article 3 Data minimisation

Researchers must limit the collection and/or processing of personal data to those items that are relevant to the research.

Article 4 Primary data collection

(a) When collecting personal data directly from a data subject for the purpose of research:

i. Researchers must identify themselves promptly and data subjects must be able to verify the identity and bona fides of the researcher without difficulty.

ii. Researchers must clearly state the general purpose of the research as soon as methodologically possible.

iii. Researchers must ensure that participation is voluntary and based on information about the general purpose and nature of the research that is adequate and not misleading.

iv. Researchers must inform data subjects if there is any activity that will involve re-contact and data subjects must agree to be re-contacted. The only exception to this is re-contact for quality control purposes.

v. Researchers must respect the right of data subjects to refuse requests to participate in research.

(b) Researchers must allow data subjects to withdraw from the research at any time and access or rectify personal data held about them.

(c) Passive data collection should be based on the consent of the data subject and meet all conditions in Article 4(a).
(d) When using passive data collection methods where it is not possible to obtain consent, researchers must have legally permissible grounds to collect the data and they must remove or obscure any identifying characteristics as soon as operationally possible.

Article 5 Use of secondary data

When using secondary data that includes personal data researchers must ensure that:

(a) The intended use is compatible with the purpose for which the data was originally collected.
(b) The data was not collected in violation of restrictions imposed by law, through deception, or in ways that were not apparent to or reasonably discernible and anticipated by the data subject.
(c) The intended use was not specifically excluded in the privacy notice provided at the time of original collection.
(d) Any requests from individual data subjects that their data not be used for other purposes are honoured.
(e) Use of the data will not result in harm to data subjects and there are measures in place to guard against such harm.

Article 6 Data protection and privacy

(a) If researchers plan to collect personal data for research that may also be used for a non-research purpose, this must be made clear to data subjects prior to data collection and their consent for the non-research use obtained.
(b) Researchers must not share a data subject's personal data with a client unless the data subject has given consent to do so and has agreed to the specific purpose for which it will be used.
(c) Researchers must have a privacy notice that is readily accessible by data subjects and is easily understood.
(d) Researchers must ensure that personal data cannot be traced nor an individual's identity inferred via deductive disclosure (for example, through cross-analysis, small samples or combination with other data such as a client's records or secondary data in the public domain).
(e) Researchers must take all reasonable precautions to ensure that personal data is held securely. It must be protected against risks such as loss, unauthorised access, destruction, misuse, manipulation or disclosure.
(f) Personal data is to be held no longer than is necessary for the purpose for which it was collected or used.

(g) If personal data is to be transferred to subcontractors or other service providers, researchers must ensure that the recipients employ at least an equivalent level of security measures.

Reflecting its intended global coverage, many of the above quoted provisions of the ICC/ESOMAR International Code state aspects ethical professional behaviour by research professionals that in Australia are regulated by provisions of Australian Consumer Law and direct operation of the Privacy Act in relation to acts and practices of APP entities.

The nature of market, opinion and social research and the role of the PMSR Code

The purpose of market, opinion and social research is to deliver information and insights about people's behaviour, needs and attitudes to inform decision making by providers of goods and services, governments, individuals and society at large.

Research approaches include:

- Research using a 'panel' of individuals or households that have agreed to be part of a panel
- qualitative and quantitative research based on free-found recruitment
- random dialled telephone interviews
- customer satisfaction surveys
- online surveys such as web based surveys and audience measurement surveys
- demographic segmentation based on research surveys
- tracking based digital market research.

Collection and processing of personal information is fundamental to the work of researchers. Diverse and evolving techniques, based on qualitative, quantitative or passive methods such as surveys, focus groups, digital measurement, wearable technologies or analytics of large data sets, enable researchers to collect and process personal data to deliver evidence-based insights to clients.

Market, opinion and social research requires robust data protection measures to build trust and meet legal and regulatory requirements. Researchers rely primarily on data collected through direct interaction with and observation of participating individuals. Research is increasingly reliant upon capture, collation and curation of information in digital form, including information derived from devices and systems. The role of the researcher is evolving from interviewer to data curator, focusing on organising and integrating data, much of which already exists. Research and insight activities are extending beyond data collection and analysis to managing and synthesising data from a diverse range of sources, from focus groups and sample surveys to social media and large databases.

However, primary source data collected through direct interaction with and observation of participating individuals remains the most important source of research data.

The depth of information about participating individuals that is required to be collected, collated, analysed and reported upon, in order to provide statistically reliable insights about a cohort of participating individuals, requires close cooperation and trust of participating individuals.

For a research organisation to gain and maintain cooperation and trust of participating individuals, controls and safeguards will need to address data privacy and other concerns as to ethical and fair business practices of the research organisation. In Australia, some concerns as to ethical and fair business practices are addressed through operation of Australian Consumer Law and in particular the ACL prohibitions addressing misleading and deceptive conduct. Good governance, and fair and ethical (as well as legal) practices and processes for managing market, opinion and social research data, require implementation of controls and safeguards in each research organisation that:

- are transparent;
- are demonstrably and verifiably reliable;
- ensure that research is carried out honestly and objectively;
- ensure that research is carried out without infringing privacy rights or expectations as to confidentiality and privacy of participating individuals; and
- ensure that research is carried out without creating detriments for participating individuals whose personal information is used in research.

- **Consent of participating individuals**

Fully informed consent of a participating individual is essential to gain and maintain trust of an individual whose personal information is being collected and handled in the course of conduct of market, opinion and social research.

Fully informed consent is required both for collection and handling of personal information about participating individuals through direct interaction with and observation of participating individuals, and through any secondary collection that those individuals may authorise (such as through online research or other use of secondary sources).

AMSRO requires all AMSRO members to accede to and comply with the PMSR Code, including those members that otherwise could claim the small business operator exemption from the requirement that APP entities comply with the Privacy Act.[28] Accordingly, the PMSR Code brings within its operation, including its requirements as to compliance and reporting as to compliance, many organisations that otherwise would not be regulated by the Privacy Act.

The PMSR Code does not activate research exceptions and exemptions from the Privacy Act. AMSRO members must only collect and handle personal information about individuals as

[28] Section 6D of the Privacy Act.

contemplated by the PMSR Code in accordance with the consent given by each affected individual.

There is no substantive equivalent under the Privacy Act to the 'legitimate interests' grounds for processing under GDPR.[29] Accordingly, the PMSR Code does not activate legitimate interests or other alternative grounds for collection and handling of personal information about individuals.[30]

The PMSR Code, and the activities of AMSRO members regulated by it, are expressly based upon consent-based collection and handling of personal information about individuals.

Individuals freely elect whether to participate, or to decline to participate, in market, opinion and social research. Consent for most modes of market, opinion and social research is not sought or obtained by click-through or other modes of signifying consent where legitimate questions may arise as to whether the affected individual has provided fully informed consent. Usually the quality of consent, and the scope of activities by the research organisation that are permitted by the consent, should be clear.

Further, and unlike many other consent-based activities of APP entities engaging in marketing of products or services, the scope of activity of the research organisation collecting and using market, opinion and social research data should be capable of explanation and exhaustive statement in terms that are readily understood.

- **Minimisation of collection and handling of personal information**

Research organisations and researchers working for them have a number of advantages over direct marketers and other commercial marketing enterprises, in relation to minimisation of collection, use, retention and other handling, and disclosure of personally identifying information about individuals.

- Research organisations and researchers should have no interest in the identity of individuals in order to take direct action toward them or to change their opinions, attitudes, or behaviours.
- Research organisations and researchers should be able to provide insights and reports to clients of the research organisations without revealing any personally identifying information about participating individuals, or otherwise providing insights and reports in any form or format which might be used by the client or any secondary recipient in any way (including through combination with other information available to the client or secondary participant) that might lead to a

[29] Contrast AFAMRO and ESOMAR, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR, June 2017, available at https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.

[30] See also Market Research Society (MRS), GDPR FAQs at https://www.mrs.org.uk/standards/gdpr-faq.

participating individual becoming reidentifiable by any recipient of the insight or report.

Further, separation of research organisations from their clients should readily enable reliable and verifiable separation of:

- data and databases of research organisations that may be linkable to personal identifiers of participating individuals, and
- data as made available by the research organisation to clients of the research organisation. That data may be made available to the client in the form of written insights or other reports, or access to data cubes curated by the research organisation and accessible by client's authorised users using client dashboards.

In whatever form data is made available by the research organisation to clients of the research organisation, this data should be reliably and verifiably deidentified before it is made available to a client of a research organisation, unless three conditions are all satisfied, being:

- that a participating individual has expressly agreed that participating individual's personal information will be shared with the client, and
- there is a compelling reason why a participating individual's personal information needs to be shared for this purpose (and use by the client is limited to this purpose), and
- there is no possible detriment or harm to the individual.

In summary, good practice in conduct of market, opinion and social research, and in managing market, opinion and social research data, should not be create risks of harms to participating individuals, or be significantly privacy affecting.

However, minimisation of handling of personal information and other good data privacy practices generally will not obviate any need for a research organisation to collect and retain limited personal information about participating individuals.

Generally, it will not be reasonably practicable for a research organisation to conduct market, opinion and social research without collection of some personal information about participating individuals. Collection and retention of personal identifiers is usually required to create and maintain an audit trail as to:

- provision of consent by participating individuals,
- data quality, and
- representativeness of the cohort of individuals within the research group.

Research organisations should manage risk of collection, use, disclosure and retention of personal identifiers and personably identifying information about participating individuals by minimising each to that which is absolutely necessary to effect the research purpose and such directly related secondary purposes.

- **Good data privacy risk management governance and practices**

The core role of the PMSR Code might be summarised as ensuring that:

- requests for consent of participating individuals are well framed and readily understood, as well as complying with all legal requirements as to fully informed consent;
- good data privacy practice is deeply embedded in the culture and business practices of research organisations;
- good data privacy practice is given reliable effect in each research organisation through ongoing and reliable implementation by that research organisation of controls and safeguards as to uses and disclosures of data that is, or could become, personally identifying;
- data privacy practice gives effect to the limitations as to scope of activities by the research organisation and uses and disclosures of personally identifying information about participating individuals that should be clearly stated in the consent provided by that individual.

Good data privacy risk management governance and practices by research organisations must address each of:

- collection and handling of raw collected data and transformation of that data into inputs for the research organisation's data analytics environment,
- separation of personal identifiers (i.e. name and other direct identifiers) from anonymisation keys or other pseudonymised transactor keys as may be used with transactor level data for analysis within the research organisation's data analytics environment,
- management of the research organisation's data analytics environment, including through deployment and monitoring of technical, operational, contractual and other legal controls and safeguards that protect data within that environment from reidentification risk and unauthorised access, use or disclosure,
- evaluation by the research organisation of the form and format in which outputs are provided to any client of the research organisation, and
- management by a research organisation of personal information (such as identifiers) to the extent that this personal information must be retained as such (i.e. in identifying form) for any of the reasons identified above.

The process of this Review

The Independent Reviewer initially consulted with the AMSRO Privacy Compliance Committee and the AMSRO Secretariat as to their experience with oversight of the PMSR Code and in dealings with AMSRO members as to privacy related matters.

The AMSRO Privacy Compliance Committee produced a draft revision of the PMSR Code for discussion with and further revision by the Independent Reviewer.

After several iterations of revisions, the draft was considered ready for release for consideration and input by interested stakeholders.

The draft revised Code was released in mark-up form (marking up all changes for the current PMSR Code) and with associated explanatory matter.

The draft revised Code and associated explanatory matter was available for consultation and input over a period from Wednesday 11 December 2019 until Friday 17 January 2020.

The Code review was notified by the AMSRO Secretariat to civil society organisations and other potentially interested stakeholders as listed in an attachment to this document.

The AMSRO Media Release is attached to this Review report.

Notifications included the following:

Name of organisation	Contact	Method	Date
Office of the Australian Information Commissioner (OAIC)	Kellie Fonseca Director Regulation & Strategy Branch	Correspondence & Meeting/s Kellie Fonseca kellie.fonseca@oaic.gov.au	Nov 2019
AMSRO member organisations	AMSRO Secretariat	Member communications Invitation to comment	6 -20 November
ACCAN	Teresa Corbin, CEO / Una Lawrence, Director of Policy	Via media Release & invitation ceo@accan.org.au	w/c 9 December
Australian Bureau of Statistics	Asst. Head of Statistics	Via media Release & invitation	w/c 9 December
Australian Privacy Foundation	Dr Roger Clarke Vice Chair	Via media Release & invitation enquiries@privacy.org.au; Roger.Clarke@privacy.org.au	w/c 9 December
Choice (Australian Consumers Association)	Alan Kirkland, CEO	Via media Release & invitation https://www.choice.com.au/ alan@choice.com.au	w/c 9 December

Communications Alliance	John Standen	Via media Release & invitation https://www.commsalliance.com.au/	w/c 9 December
Consumers' Federation of Australia (CFA)	Gerard Brody (Chair) *& CEO of the Consumer Action Law Centre*	Via media Release & invitation standards@consumeraction.org.au	w/c 9 December
Consumers Health Forum Australia	Leanne Wells, CEO; James Ansell, Research & Policy Officer	Via media Release & invitation info@chf.org.au	w/c 9 December
Consumer Policy Research Centre	Lauren Solomon, CEO	Via media Release & invitation https://cprc.org.au office@cprc.org.au	w/c 9 December
Industry organisations – AMSRS, ADMA, AANA, The Data Institute, AMI & IML	CEO/Chairs	Via media Release & invitation amsrs@amsrs.com.au comply@adma.com.au admin@aana.com.au info@thedatainstitute.com.au Narendra.Prasad@ami.org.au david.pich@managersandleaders.com.au	w/c 9 December
Trade Media publications – Mumbrella, B&T, CMO, SMH, The Australian, The Financial Review, MR Webb, Daily Research Business, ESOMAR, GRBN	Rochelle Burbury Third Ave PR	Media Release	w/c 9 December

The revised draft Code[31], the Independent Review and the intent of the Independent Review[32] were also publicised on the OAIC website[33] and on the AMSRO website[34].

Two submissions were received from interested parties.

Their input is discussed below, together with the further revisions made to the Code to address that input and other suggestions by AMSRO members as to improvements to the draft released for consultation.

OAIC's requirements

The OAIC Guidelines for developing codes[35] relevantly provide:

> 1.5 The purpose of a code is to provide individuals with transparency about how their information will be handled. Codes do not replace the relevant provisions of the Privacy Act, but operate in addition to the requirements of the Privacy Act. A code cannot lessen the privacy rights of an individual provided for in the Privacy Act. Registered codes are disallowable legislative instruments.
>
> 1.6 An entity bound by a registered code must not do an act, or engage in a practice, that breaches that code (ss 26A (**APP codes**) and 26L (**CR code**)). A breach of a registered code will be an interference with the privacy of an individual under s13 of the Privacy Act and subject to investigation by the Information Commissioner under Part V of the Privacy Act.
>
> 1.7 As a breach of any provision of a registered code is an interference with the privacy of an individual, a code should limit itself to provisions which outline the specific obligations of entities' bound by the code. For example, for APP codes this would cover obligations to apply or comply with one or more APPs or to meet higher standards of personal information handling than required by one or more of the APPs. It would also cover governance or administrative items that must be included in a code (s26C(2)), or which are directly related to the handling of personal information by entities bound by the code. Other administrative and governance issues should be dealt with separately (see Part 3 on Code governance).
>
> …….
>
> 1.11 The primary purpose of an APP code is to set out how one or more of the APPs are to be applied or complied with. An APP code may also impose additional

[31] https://www.amsro.com.au/privacy-code-review-2019/#_ftn1
[32] https://www.amsro.com.au/amsroresp/wp-content/uploads/2019/11/AMSRO-Code-Review-2019-Explanatory-Notes-.pdf
[33] https://www.oaic.gov.au/updates/news-and-media/independent-review-of-the-privacy-market-and-social-research-code-2014/
[34] https://www.amsro.com.au/privacy-code-review-2019/
[35] Available at https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-for-developing-codes/.

requirements to those in the APPs and/or cover certain exemptions. As such, reasons for developing an APP code may include:

- providing greater clarity of how particular APPs are applied or complied with in a specific industry context or in relation to new and emerging technologies which entities bound by the code utilise
- incorporating higher standards for privacy protection than the Privacy Act requires, including covering certain exempt acts or practices or providing for additional obligations to those in the APPs or Part IIIA
- assisting in promoting cultural change in an industry sector in relation to personal information handling.

1.12 In deciding whether to develop an APP code, an entity should also consider:

- whether existing legislation, regulation or a code covers the same or similar topics that may negate the need to develop an APP code or may be suitable for adoption without the need to develop a separate APP code
- whether entities that will be bound by the APP code have sufficient resources to implement the code's requirements and whether there are sufficient resources available to develop and administer the APP code.

Under APP 1.2, all APP entities must have practices or procedures in place to deal with complaints or enquiries from individuals about the entity's compliance with the APPs and any APP code they are bound by. An APP code developer should include, as part of the ongoing code governance, mechanisms for a code administrator to monitor the code's effectiveness in achieving compliance from entities bound by the code.

……..

3.16 To assist a code administrator to monitor the compliance of entities bound by an APP code, the APP code should require bound entities to provide an annual report to the code administrator. These annual reports should outline how the entity is complying with the code including the number, nature and outcomes of any complaints about the code made to the entity. More specifically, such a report could include:

- the number of complaints in relation to the code received in the financial year
- statistical information about the nature of the complaints (e.g. the number of complaints related to specific code provisions or APPs)
- the average time taken to resolve the complaints
- statistical information about the outcomes of complaints (e.g. conciliate, withdrawal, referrals to an EDR scheme)
- statistical information about the remedies awarded in finalising the complaint (e.g. compensation, apology, staff training).

3.17 These reporting requirements should be undertaken in a way that minimises the burden, for both the code administrator and the entities bound by a code. It is anticipated that reporting should be achieved through simple collection, aggregation and reporting methods. However, the methodology used to complete these reporting requirements will be determined by the code developer when drafting the code.

3.18 To further assist in monitoring compliance, code developers may also include a standardised internal complaint handling system to be adopted by entities bound by the code (see Part 4). Also, where relevant, consideration could be given to including a risk based system for auditing for serious or repeated interferences with privacy or systemic issues related to compliance with the code.

4.1 APP entities are required to take reasonable steps to implement practices, procedures and systems to deal with privacy-related inquiries or privacy complaints from individuals, including in relation to a registered code that the entity is bound by (APP 1.2). The Information Commissioner generally expects that an individual's privacy complaint will follow a three-stage process:

- The individual first makes a privacy complaint to the APP entity.
- If the individual is not satisfied with the outcome, the individual may make a privacy complaint to a recognised external dispute resolution (EDR) scheme of which the APP entity is a member.
- If the APP entity is not a member of a recognised EDR scheme, or the individual is not satisfied with the outcome of the EDR process, the individual may make a privacy complaint to the Information Commissioner under s 36 of the Privacy Act.

……

Part 6 – Reviewing, varying and removing registered codes

Review of registered codes initiated by a code administrator.

6.1 The governance arrangements for both registered APP codes and the CR code should include a code administrator initiating regular independent reviews of the operation of the code. This will ensure the code remains effective and relevant (see paragraphs 3.4–3.5). A code review should be overseen by a suitably independent person and where practicable supported by a steering group which should include at least one representative from a relevant consumer group.

6.2 An independent review of a code should:

- occur at regular intervals, at least every 5 years, and have a scope broad enough to capture all potential issues related to the code's effectiveness and relevance

- include a public consultation process with relevant stakeholders (e.g. entities bound by the code, individuals who transact with those entities)
- result in a report made publicly available online which outlines:
  - ➢ the issues raised by the review
  - ➢ the findings of the review
  - ➢ the actions taken, or that will be taken, by a code administrator and/or the entities bound by the code to address issues identified by the review.

6.3 A code administrator may also decide to initiate an independent review of a registered code before a regular review is due. For example, a code administrator may initiate an independent review if an audit indicates a lack of compliance with the registered code (see paragraphs 3.18 and 3.19) or a code administrator becomes aware of systemic issues that would justify a review.

Input and response

Two written submissions were received by AMSRO, from the Australian Privacy Foundation (**APF**) and from the Australian Market & Social Research Society Limited (**AMSRS**).

The following table addresses comments made in those submissions.

Subject matter and submitter	Comment	Response by AMSRO	Recommendations by Independent Reviewer and Action Taken
Coverage - APF	While AMSRO members are understood to be obliged to adopt the Code, membership of AMSRO is not mandatory, and a case can be made that community interests would be better served by amendment of the Act to cover all market and social researchers, rather than relying on an optional self-	As the APF later notes, self-reporting by Code members and active administration of the Code by the Code Administrator are important elements of Code. AMSRO as Code Administrator would not have ability to ensure reliability of self-reporting or other aspects of compliance with the Code to the extent	Non-AMSRO members could elect to adhere to provisions of the Code. In this sense the Code is not exclusionary of any entity. However, given the responsibilities of a Code Administrator to ensure Code compliance, it is not realistic to expect a Code Administrator to exercise jurisdiction over

	regulatory Code that does not have comprehensive coverage of relevant research entities.	that the Code purported to apply to entities that were not members of the Code. Further, by the condition of membership of AMSRO, AMSRO extends the operation of the Code to small business operators that otherwise are exempted from coverage of the Privacy Act. The OAIC could not mandate that SBOs comply with the Code.	entities in relation to whom it does not have any authority to enforce compliance with the Code. AMSRO membership provides the necessary link between the Code and ability to enforce the Code, and the funding that AMSRO requires to actively administer the Code.
Scope of Review - APF	In conducting the Review Professor Leonard has only proposed minimal – largely cosmetic – changes updating the Code for changes in the law and circumstances. Given his limited charter, the Review does not provide a meaningful critique of the regime.	The charter granted to the Independent Reviewer was not relevantly constrained.	The Independent Reviewer did not regard the Terms of Reference as constraining ability to address concerns with any of the existing provisions of the Code or to look outside the Code for examples of good practice in other jurisdictions. The Code was reviewed in the context of other regulations affecting research including provisions of the Australian Consumer Law and the jurisdiction of the ACCC to enforce those provisions,

			and standards and other codes.
Reporting - APF	The Code is vitiated by an inherent and substantive weakness in reporting. That raises questions about whether the regime has been and 'remains effective and relevant'.	AMSRO members are required to self-report systemic issues or serious or repeated breaches of the Code to AMSRO, and AMSRO to investigate and publicly report on such breaches. The AMSRO Secretariat is not aware of any circumstances where an issue that may be a significant breach of the Code (or otherwise a breach of the Privacy Act) has not been reported to AMSO because it has not been considered a systemic issue or a serious or repeated breach. The AMSRO Privacy Compliance Committee includes consumer and independent representatives and informs itself of AMSRO member practices inquires of industry representatives, training programs and logged queries in the AMSRO	It is not usual for a Code to require reporting of any possible breach however insubstantial. The formulation of "systemic issues or serious or repeated breaches of the Code" is subjective, but relatively common. Having regard to the APF's submission, the Independent Reviewer recommends a clarification to the Code such that if a research organisation is in doubt as to whether an issue is systemic or serious, it is directed to self-report. See highlighted further amendment in the Further Revised Code.

		member query register. AMSRO and the PCC also led a member consultation Code Review phase ahead of the public phase (6 November to 20 November).	
Reporting by AMSRO	These Reports only superficially engage with implementation of the Code, i.e. the practical experience of AMSRO – see Code F(e) and H(e). In particular, the Reports do not provide external stakeholders with information about whether any aspects of the Code are causing concern or complaints, and thereby require attention in the review.	Absence of reporting to external stakeholders about whether any aspects of the Code are causing concern or complaints is not an indication of failure of monitoring as to whether any aspects of the Code are causing concern or complaints.	The annual reports should specifically address whether any aspects of the Code are causing concern or complaints, if only to note (if this is correct) the absence of any concerns or complaints known to the AMSRO Secretariat or the PCC during the review period in question, having made reasonable enquiries of AMSRO members.
Input from AMSRO members as to their experience operating under the Code - APF	The Foundation is not aware of whether AMSRO facilitated examination by the reviewer of member experience. Examination through contact with representative members is essential to validate the reports and thereby underpin	This concern could be addressed through an annual survey of AMSRO members, as part of Code monitoring.	An annual survey would provide AMSRO with a better evidence base for Code administration. A change to the Code to mandate an annual feedback review is recommended - see highlighted further amendment in the

	the legitimacy of both the Review and the Code.		Further Revised Code.
Self-reporting under the Code by AMSRO members - APF	The Code requires AMSRO members to report any serious or systemic issues. That requirement under H(e) also requires members to report any serious and repeated breaches of the Code. Eligible data breaches are addressed under H(b). The reports are read as indicating there have been no serious or systemic issues or breaches in the past five years, and that there have been no complaints reported to the Code Administrator under clause H(a). The Foundation is concerned that a complete absence of complaints is at odds with experience in other countries and thus somewhat implausible.	See above.	See above. There is not asserted to be a ''complete absence of complaints" to AMSRO members. The Independent Reviewer is not aware of any evidence base as to "comparable experience in other countries.
Transparency regarding contact with research entities - APF	There is an ongoing lack of transparency regarding contact with research entities. The Foundation notes that the Explanatory	Here was no intent to 'obfuscate' on this point: only a desire to ensure that small AMSRO members that did not have mature	The AMSRO response is noted and addressed: see highlighted further amendment in the Further Revised Code.

	Note (EN) regarding Code item 5.2(a) remains unchanged, allowing research firms to give an AMSRO email address as the point of contact. The rationale for such obfuscation is unpersuasive, and the Code must be amended to provide for a clear direct entity-specific point of contact, as well as the AMSRO point for further inquiries.	processes and systems for complaint handling could offer a suitable alternative such as directing complaints to AMSRO. The drafting should be clarified.	
Requirement to disclose client identity - APF	The 'extra' requirement to disclose client identity is unchanged. However, there has been no change to the 'exceptions', and AMSRO reporting regarding the Code provides no substantive data about this potentially important area of practice. It is unclear how frequently research entities are claiming these exceptions to conceal the identity of the client, for what purpose, and at what scale (a handful of individuals or a	The relevant substantive text in the Code reads "Research Organisations must disclose the identity of the client, unprompted, no later than the end of the collection of information, except where the Research Organisation and client have reasonable grounds to decide that there are genuine research concerns or where there is another compelling reason not to do so (e.g. it may expose one of the parties to legal action)." The APF's request for reporting as to the	The Explanatory Note was confusing and the substantive text that was purportedly explained is clear. The amendment is sensible. A change to the Code to mandate an annual feedback review is recommended - see highlighted further amendment in the Further Revised Code.

	much larger population).	use of exceptions could be accommodated through an annual survey of AMSRO members as part of Code monitoring.	
Deletion of the Explanatory Note in the Code regarding the 'permitted health situations' exception - APF	Explanation of this is necessary, given the significance of Privacy Act 1988 (Cth) s 16B (2) of the Act which covers the very limited circumstances under which such an exception will be founded. It is understood that the sort of market and social research covered by the Code would rarely overlap with medical and health research, which is normally conducted under a much more stringent ethical governance regime.	The APF's understanding is correct and AMSRO's expectation is that permitted health situations will rarely, if ever, be relevant to research conducted pursuant to the Code.	Noted: the definition of 'genuine research concerns' appears adequate to describe the disclosure circumstances as contemplated by the Code, and other statutory exceptions will operate on their face in the rare circumstances where those exceptions may operate. Detailed guidance is already available as to the statutory exceptions, including in the OAIC Australian Privacy Principles guidelines.
AMSRS Code of Professional Behaviour - AMSRS	The AMSRS Code of Professional Behaviour includes issues of privacy and data protection, but has a broader focus, covering the professional behaviour of members and their responsibilities to participants in	Agreed. However, because the AMSRS Code of Professional Behaviour is not administered by AMSRO, AMSRO is unable to ensure reliability of self-reporting under the AMSRS Code or other aspects of compliance of	Given the responsibilities of a Code Administrator to ensure Code compliance, it is not realistic to expect a Code Administrator to ensure compliance with a Code that it does not administer.

	research. The AMSRS Code of Professional Behaviour is a key part of a self-regulation framework and includes a formal complaints process.	individuals and other entities subscribing to the Code.	
Broadening of the scope of the Privacy Code - AMSRS	AMSRS proposes a broadening of the scope of the Privacy Code, designed to benefit a greater number of organisations providing research services in Australia. We see this as extending the efficacy and relevance of the Privacy Code. We have recently introduced two new categories of membership: Company Partners and Client Partners. We propose that AMSRO consider extending the scope of the Privacy Code to cover our Company Partners. This would provide a clear benefit in further extending the industry privacy regime that provides assurance of protection of personal	AMSRO agrees that there would be value for the industry and for the public for the coverage of the code to be expanded to include the 40 AMSRS Company Partners that are not currently AMSRO members. In addition to greater privacy protection for the public (research participants), this would reduce the risk of reputational damage for the industry from poor privacy protection practice among companies in the industry. However, the path proposed by AMSRS to achieve this benefit is inequitable to existing AMSRO members and would likely reduce incentives for	Non-AMSRO members could elect to adhere to provisions of the Code. In this sense the Code is not exclusionary of any entity. However, given the responsibilities of a Code Administrator to ensure Code compliance, it is not realistic to expect a Code Administrator to exercise jurisdiction over entities in relation to whom it does not have any authority to enforce compliance with the Code. AMSRO membership provides the necessary link between the Code and ability to enforce the Code, and the funding that AMSRO requires to actively administer the Code.

	information to the public. We currently have 61 Company Partners with some limited overlap with AMSRO membership (21 are members of both organisations). Our proposal would therefore bring a further 40 organisations within the scope of the Privacy Code.	prospective members to join AMSRO and thereby provide AMSRO with the funding necessary to enable AMSRO to properly discharge its responsibilities as Code Administrator. AMSRS Company Partners that are not currently members of AMSRO already have a straightforward and cost-effective path to obtaining coverage under the Code (by becoming AMSRO members). Many AMSRS Company Partners (over 20) are already concurrently members of AMSRO.	
Monitoring and recording system of AMSRS	We would set up a monitoring and recording system mirroring that mandated by AMSRO for its members, outlined in Section H of the Privacy Code.	AMSRS can do so if it so wishes.	Noted.
Relationship between Code and AMSRS Code of Professional Behaviour - AMSRS	We note that all AMSRO members are bound by the Privacy Code but that not all AMSRO members include an AMSRS member (thus confirming	The Code of Professional Behaviour is not referenced in the new draft, and should not be, as AMSRO has no control over its	See last substantive comment above.

	their adherence to the AMSRS Code of Professional Behaviour). Given that the Privacy Code refers to the AMSRS Code of Professional Behaviour, we ask the reviewer to consider making adherence to the AMSRS Code of Professional Behaviour mandatory for AMSRO members, reinforcing the professional standards underpinning the Privacy Code.	content and does not now believe it is appropriate to give a voluntary professional code quasi-legislative force by virtue of its inclusion in the new version of the Code.	
Review of the AMSRS Code of Professional Behaviour - AMSRS	We are currently conducting a review of the AMSRS Code of Professional Behaviour, with a revised version due for launch on 2 March 2020. We ask that the Privacy Code review include an analysis of the revised AMSRS Code of Professional Behaviour when it becomes publicly available, to ensure that the Privacy Code references to the AMSRS Code of Professional Behaviour remain current	References to the AMSRS Code of Professional Behaviour have been deleted for the reasons above noted. AMSRO continues to strongly support the AMSRS Code of Professional Behaviour and it is an important element in the AMSRO "Privacy Quality Ethics" Trust Mark scheme. AMSRO looks forward to providing constructive input into the proposed revision of the	The AMSRO response is noted – no further action is recommended in relation to the drafting of the Further Revised Code.

		AMSRS Code of Professional Behaviour.	

Recommendations of the Independent Reviewer

1. The Revised PMSR Code as released for comment be further revised to address the additional matters identified in the above table of comments and responses. See the attached Further Revised Code. For ease of reference, all previous mark-up of changes from the current PMSR Code have been retained, and only further changes appear as mark-up and also highlighted.
2. The PMSR Code is not as prominently displayed on the AMSRO website as would be desirable. A review of the display and linking on the AMSRO website would be desirable.
3. Some of the discussion of the AMSRO "Privacy Quality Ethics" Trust Mark scheme on the AMSRO website introduces confusion as to whether compliance with the PMSR Code is an additional requirement of qualification to apply the AMSRO "Privacy Quality Ethics" Trust Mark or (as is correct) a condition to AMSRO membership (independent of qualification to apply the AMSRO "Privacy Quality Ethics" Trust Mark). This discussion should be clarified.
4. The AMSRS Code of Professional Behaviour addresses ethical and professional conduct concerns that are outside the scope of data privacy concerns as addressed by the PMSR Code. This is appropriate and reasonable, particularly given the limitations under the Privacy Act as to the scope of registered codes under that Act (that relevantly preclude adoption of a comprehensive code approach akin to the ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics). However, overlap between the two Codes potentially leads to confusion as to what subject matter is appropriately covered by which Code. AMSRO and AMSRS should work together to ensure that there is no confusion as to how the two Codes work together. AMSRO members should take care to ensure that their published material, including but not only content on their respective websites, accurately describe the two Codes.
5. AMSRO members should be reminded of the need to publish a prominent notice as to coverage of the Code and the ability of concerned persons to make privacy-related queries or complaints to the concerned AMSRO member, AMSRO and/or the OAIC, as the person elects.
6. AMSRO members should be reminded of the need to publish appropriate contact details to readily enable members of the public to address queries or concerns that are within the scope of operation of the PMSR Code.
7. Annual reporting of AMSRO as to ongoing monitoring and oversight of the PMSR Code be informed by additional enquires made by AMSRO of its members and

include additional coverage as suggested above (reflecting relevant input of the APF in in manner described in the table above).

8. Given the importance of clear and fully informed consent of participating individuals as a basis for research covered by the PMSR Code, and having regard to changing best practice in relation to privacy notices and privacy consents, AMSRO should develop further materials (including consent templates) and training for AMSRO members as to current global best practice in presenting relevant material that informs an individual in that person's decision to give or withhold consent.

Professor Peter Leonard
6 March 2020

Appendices:

AMSRO Media Release

Australian Privacy Foundation submission

Australian Market and Social Research Society submission