Australian Computer Society Inc. (ACT)
ARBN 160 325 931
National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Government of South Australia,

Department of the Premier and Cabinet

ACS submission on the South Australian Data Strategy Consultation Paper

11 March 2021

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical discussion.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology (ICT) sector, with over 48,000 members nationwide. We are passionate about the ICT profession being recognised as a driver of innovation and business – able to deliver real, tangible outcomes.

Working with our Data Sharing Committee, which is comprised of nationally recognised experts in the field of data sharing and security, we have developed a response to the questions posed in the SA consultation paper, which we hope will be useful as SA continues its already stellar work to make the most of the opportunities afforded by data sharing.

Of all the recommendations we have provided here, one of the most important take-aways is the belief that the community must be involved at all stages of any data sharing project that will involve personal data. This can be hard, and ACS is more than willing to provide assistance if needed.

Thank you so much again for your time and the opportunity to comment on this paper, and we'd be delighted to discuss this response and its proposals with you further. If you'd like to discuss any part of this response or simply seek further clarification or input, please feel free to contact myself by email at troy.steer@acs.org.au or by phone on 0417 173 740.

Yours sincerely

Troy Steer

Director of Corporate Affairs and Public Policy

Australian Computer Society

Theme 1 – Collaboration

1. Can you provide some examples of good data collaboration? What made it successful? How have these contributed to creating value?

There are two excellent examples of the South Australian government benefiting from the collaborative sharing of sensitive data, both in a multi-sectoral and multi-disciplinary manner. These are the nationally recognised work undertaken by the Registry of Senior Australians (ROSA), located within the South Australian Health and Medical Research Institute (SAHMRI); and the BEBOLD (Better Evidence Better Outcomes Linked Data platform, formerly BetterStart) research program led by Professor John Lynch at the University of Adelaide.

Both of these examples involve active partnership and collaboration in the safe sharing of sensitive information across the government and non-government sector, delivering benefits to citizens as well as government.

The South Australian Government should to be congratulated on investing $4m in 2017 through the Premier's Research and Industry Fund (PRIF), which enabled a wide range of stakeholders from the government and non-government sectors to assist the ROSA team. This has resulted in high-calibre insights, skills development and a valuable monitoring and evaluation capability of publicly funded aged care services both in SA and nationally.

Following the vision and funding that initially established ROSA, it has generated nearly $10m in additional funding, with ROSA partnering with a range of organisations nationally based on its expertise in collaborative data sharing.

To the credit of SA and the ROSA team, the Federal Royal Commission into Aged Care Quality and Safety were so impressed by the integrated data analysis performed by the ROSA team's study of the aged care sector and individual citizen outcomes that it contracted the ROSA team to analyse aged care services and outcomes across Australia, bringing together linked data from Queensland, NSW and Victoria as well as SA.

The University of Adelaide's BEBOLD (formerly BetterStart) research program is another nation-leading example of what can be done by collaborating with government and non-government partners to safely share sensitive data. The program is able to protect citizens' privacy while accurately monitoring their use and the effectiveness of government funded services and interventions, tracking outcomes from integrating government and non-government data.

It was so successful that the BEBOLD team has been asked consult with other state governments and has prepared over 100 reports to governments based on the linked data, skills and capabilities developed in the program.

BEBOLD's success was achieved using privacy-protecting and ethically approved data linkage practices pioneered in WA but developed nationally through the Australian Government NCRIS funded Population Health Research Network.

The BEBOLD program was only possible through the partnership, trust, and support of a range of government and non-government organisations that were willing and able to share their sensitive data, and the result was a leading analytical capacity based in South Australia with national influence and impact.

With BEBOLD and ROSA as examples of what can be done, the challenge for SA and Australia is how best to scale and invest in digitally-enabled sharing of sensitive data in a way that protects privacy. ACS has been working on this problem for a number of years now, and in partnership with the CSIRO's Data61 we have developed the Personally Identifying Factor as an empirical measure of privacy risk when sharing data, with

consideration of AI and the increase demand for near real-time integration and analysis of data. This work is detailed in three reports available for download on the ACS website (acs.org.au): *Data Sharing Frameworks* (September 2017); *Privacy In Data Sharing - A Guide For Business and Government* (November 2018); and *Privacy-Preserving Data Sharing Frameworks* (December 2019). We can provide PDFs or hard copies of these reports on request.

As much as anything, the barrier to safe data sharing is not technology, but people. It is essential that people's hearts and minds are engaged in the digitally-enabled future of Australia. A community focus is required, as seen in the ROSA and BEBOLD projects. Governments needs to be capable and resourced with skilled people able to collaborate with the non-government sector to address the hardest challenges of data sharing. There is value in actively promoting examples like ROSA, whose governance processes and community engagement is first class.

2. How might the SA Government improve collaboration with your agency or sector?

We recommend utilising and evolving the National COVID-19 Coordination Commission that was set up in 2020 as a part of the pandemic response. This provides a forum (not just for government agencies) and is held at regular intervals to discuss and take action on matters of national importance.

While we understand that this board now meets every month (previously it was on a day-to-day basis), it worked because it allowed for relationship building and ideation. Other peak governance committees typically only meet twice a year, allowing little time for these activities and producing few opportunities for innovation. It is important to also add that cyber security is also addressed through this group.

In addition to a proposed expansion of the Terms of Reference for the National Coordination Commission, we recommend incentivising and encouraging agencies to use data.gov.au as a platform for active collaboration and data sharing.

We also recommend the establishment in SA of a jurisdictionally-based community and consumer data advisory body with members from regional South Australia who would augment the more formal national coordination capability. This would provide insight and direction on data sharing and use from a community perspective across SA.

Theme 2 – Governance

3. What are the challenges to good data governance in your organisation? What has helped and what would you recommend to others?

Some of this is addressed in the response to question 2 above – there's a need to include a community and consumer advisory capability that is currently lacking (nationwide), but extremely important as more data-driven digitally enabled services are being considered and implemented.

Secondly, it's essential to address the lack of knowledge with respect to what data is captured and what variables within a data source can be relied on. This requires effective data ownership and stewardship, with data custodians able to consistently record and publish searchable metadata – otherwise the source of truth is lost.

Acknowledge that good governance starts with the identification and assignment of responsibilities to a data owner and a delegated data custodian for each data source. This top-down approach assigns clear responsibilities and obligations to the wider community on the benefits of data sharing and complements a bottom-up training and empowerment approach.

Having common and agreed terminology is also essential for good governance. Peter Christen from ANU and internationally renowned Privacy Protecting Bloom Filter Expert Rainer Schnell from Germany, who along with Peter's ANU colleague Thilina Banbaduge recently released a particularly useful book that includes a glossary, built up over the past 2 or 3 decades.

The appendix of the book *Linking Sensitive Data* contains has a very practical glossary of terms, describing most of the terms that are useful in explaining data access and use. The book is available to order or preview at: https://www.springer.com/gp/book/9783030597054.

Importantly, on page 403 there are several useful definitions including Data Custodians, Data Owner (referred to as Database Owner), Data Controller and Data Provider. We would strongly recommend that SA Government considers using this work as a platform as it builds towards a standardised approach to data sharing.

When it comes to building the data platforms themselves, we also recommend relying upon a standardised approach, which will ensure improved data accessibility and management. At present, there is a fundamental issue of inconsistent and non-searchable metadata at a field/variable level across various agencies and organisations.

Rather than developing bespoke metadata engines and metadata repositories within the SA Government, the nationally relevant and continually updated and improved AIHW searchable Metadata Online Registry (METeOR) should be mandated for use, and supported to be expanded to manage more than national minimum datasets.

4. What might system wide governance and leadership look like and mean to you?

Governance and reform must start from the top. There needs to be leadership and clear guidance with respect to the opportunity and obligations for data sharing, particularly the data that has been collected by public organisations, and also non-government organisations that has been funded or part-funded by public monies. As is the case in the United States Federal Government, where organisations receiving public monies are obligated to make privacy protected data available to be linked and used for integrated analysis and research benefiting the public.

Therefore to stimulate both social and economic benefit in South Australia, as well as Australia wide, consideration should be taken to mandating the obligation on organisations to make the data available, when providing services to the community that have been fully or part funded by public monies. As such, data funded by public monies would be treated as a community asset, with an obligation for it to be shared. This would drive expectations on data access and use and develop a culture that would support a digitally enabled future for Australia.

However, the implications of the misuse of that data will need to be addressed in the reforms being considered in the Privacy Act 1988 (Cth) and the Data Availability and Transparency Bill introduced into the Australian Parliament on 9 December 2020. Technology companies, state-based actors and criminal syndicates are already using public data, and as a nation, we need to move quickly to both empower and protect the community with respect to the access and use of sensitive data. That will require SA to work nationally with all jurisdictions on these issues.

Theme 3 – Security

5. How might your data security practises be improved? What challenges do you face with enforcing data security standards?

As mentioned in the response to question 3, a good starting point is enforcing consistent terminology, which will help promote greater understanding and the adoption of standards. Given the current wide range of data regulations and potentially evolving standards, the development of a consolidated and actionable framework, including data security and privacy, based on these regulations and standards would promote better understanding, reduce duplication and cost.

Importantly, data needs ownership to ensure its source and authenticity, providing assurance of its accuracy and security. In addition, we would also recommend a system or dashboard where citizens can see their data and who has been given access to it. This would provide greater assurance to citizens and the community, building and demonstrating trust in businesses and governments.

6. How do you ensure the proper classification of data?

Given the existing Australian Government Protective Security Policy Framework (https://www.protectivesecurity.gov.au/) and the Information Security Manual (ISM) that underpins it, the challenge faced nationally is how best to make these policies and practices broadly accepted and understood.

For the SA Government, a focus needs to be on producing colourful and engaging one-page explanatory pieces that can be used to drive the necessary behaviour and outcomes. A well-designed information flyer and associated education program would help to convey the varying levels of personal information, health information, financial information, and others types of information, in a way that organisations and their staff can easily apply.

To enforce proper classification, this education plan could be combined with practical tools. Quality criteria-based tools that could be used to automatically classify and detect potential classification omissions and errors would be highly useful, for example.

7. How do you ensure data that has been on-shared to third-parties remains safe and secure?

It is extremely difficult to control data once it has been shared. From a practical perspective, trust is invariably going to be a key factor in any sharing scheme. The key is how to quantify and verify trust. For example, once data is viewed on a screen, a camera could take pictures of the screen, effectively breaking the IT-based security protocols. The information in the photo image is now out of control, outside of the password and other IT security mechanisms designed to prevent unauthorised access and release.

Therefore it's necessary to have the IT controls, training and security awareness, and combine them with controls such as deeds of confidentiality and compliance that prevent the adding or sharing of data provided. So who and how do you accredit individuals and organisations as trusted parties able to be responsible for accessing the using sensitive and confidential data and systems?

The Data Availability and Transparency Bill, introduced into Australian Parliament on 9 December 2020, is designed to address this issue of accreditation of trusted parties.

On an organisational level, the ACS stipulates and maintains a professional code of ethical conduct for members. This is comparable to what the SA Government employees have through the Public Sector Code of Ethics, noting penalties for SA Public Servants of up to seven years in jail for deliberately releasing data without authorisation. This compares to two years in jail in the Australian Federal Government.

Having the data shared in a de-identified (potentially re-identifiable) format is manageable but challenging. This is accomplished by controlling the analytical platform or IT environment that sensitive data would be stored and analysed in. Obviously having a non-internet network, like that used by the Singapore Government, would be ideal in restricting the risk of external hacks, but the key vector for unauthorised access and release is people. People accidently or deliberately avoiding controls is an ongoing risk that needs to be managed through a range of measures and controls, including security awareness and ongoing education, accreditation and training, compliance monitoring and penalties, deeds of confidentiality and codes of ethics.

The Australian Finance Industry is a useful case study of where sensitive financial data is shared, often without explicit consent, for example when seeking a loan.

Based on the principle that data about an individual, collected using public resources or private resources belongs to the individual (noting this not the case in Australia due to intellectual property law assigning property rights to the author of a records, not the subject of the record), then a person's data can be considered valuable and rather than contemporary data sharing occurring, where the individual or citizen is unaware and not informed when records on themselves are being shared and used, a new approach of smart data sharing could be considered. This would be respectful of a person's right to know who is receiving data about them and for what purposes.

The value of a person's data currently does not provide a direct benefit back to the individual, but is seen as a community benefit, where there is a public benefit from the sharing of data. It may be possible using smart data sharing for an individual to not only be made aware of where and who is using their data, but there could be a reward system generating credits or token when a person's records are accessed and used. This would establish an economy for the sharing data, and be positioned to start to attribute value back to the individual whose data is being used.

8. How well do you think data security standards are enforced? When was the last time you reviewed your practices and what guidance/help do you think would be beneficial?

Data security monitoring and compliance to security policies and procedures is essential to ensure the trust of the community and citizens. Regular independent audits also provide a business process improvement capability. We cover this is our response to question 7 above.

Theme 4 – Innovation

9. How might government and industry make the best use of data to grow the economy? What are some examples and what some of the barriers?

A key generator of value is to use the data to support government activities. The excellent COVID-19 response in certain jurisdictions increased the volume, scope and frequency of data being shared and linked. This enabled flight manifests and shipping passenger and crew lists to be linked overnight to a wide range of data sources through the respective jurisdictions' linked data system co-funded by the Australian Government NCRIS PHRN data sharing infrastructure.

COVID-19 has seen an increase in the amount and range of data being shared. However, the underpinning constraints and issues remain, being the lack of skilled data people, competing priorities, lack of consistent and variable-level metadata, reluctance to share particularly if the quality of the data can be called into question, and siloed organisational responses.

For effective interoperability and re-use, the importance of Standards, in particular, the ongoing importance of aligning data activities and development with standards able to promote secure data access and use of sensitive data across both jurisdictional governments and the non-government sectors is essential. The ACS stresses the importance for SA Government, and all of the government sectors to actively engage and participate in the international standards developments, specifically JTC 1/SC 32/WG 6 – Data Usage.

10. What role can the tertiary sector play in enabling data driven innovations? What are some examples?

The tertiary sector is a key resource that government and the wider community can draw on. The case studies provided in the response to question 1 above (ROSA and BEBOLD) were directly enabled by the university sector.

This highlights the capability of the tertiary sector to add value, drive and in fact create new services and opportunities that government alone could not realise. Therefore upskilling and investment in the tertiary sector is essential in driving forward Australia's digitally-enabled economy.

The ability of the SA Government to partner and target key areas of potential growth, job and economic development is recognised as being tricky, and with national competition from other jurisdictional governments and the private sector. This will take persistent engagement and relationship building to deliver a sustainable competitive advantage for the state. The provision of skilled and knowledgeable ICT across all levels of education is an investment in the future prosperity of the South Australian community and the nation.

11. In what areas of the South Australian Government are there the biggest opportunities for data innovation?

Attention needs to be given by governments to bringing the citizens and the wider community into the conversation about how their data is used, and where the citizens' data should be used. From a government perspective, good data governance builds trust with its citizens. Unfortunately, the need for

citizen representation in all discussions around data and information is often not adequacy or consistently considered, particularly within operational government agencies.

To be a national leader it would be useful for SA to form a citizen jury, formally established not for decision making but for effective engagement, consultation and advice, particularly in the use of digitally enabled services using publicly funded data. The ACS is the national peak body for the technology professions and we would welcome the opportunity to convene a sponsored body, able to engage with the broader community and be a positive force for government-funded development of digital information systems and digitally-enabled services.

Such a body would be a key advocate and voice for the community and can be positioned to be independent promoters of the benefits and good stewardship, able to advocate and speak for the range of stakeholders including government, should issues arise from the sharing people's data.

Broadly, we encourage the SA Government to continue to lead the nation in publicly funded linked data analysis in partnership with the non-government sector, using best practice privacy protecting practices. This will have benefits both within the state and nationally. For example, the protection of children requires a national (inter-jurisdictional) data sharing capacity for placement and concerns – with seed funding of initiatives from government, able to progress a 360 degree view of the child and determinants, including child protection, youth justice, education, community and mental health, employment and training, as well as welfare and social services.

Greater availability of data will also assist the startup community and industry development. This would also encourage SME growth and innovation in the local economy.

Theme 5 – Skills & Literacy

12. What do you believe the value of data is to your organisation? How do you promote this value to staff?

One approach is to provide examples to staff of where their work, effort and activities have had a positive impact and benefit to the wider community, outside of their organisation. Guest speakers could be invited to staff meetings and talk about the importance of their work and the benefits arising.

13. How might data skills and literacy be improved in your organisation? What does a data literate workforce mean to you?

Executive engagement and understanding is important. An assessment of an organisation's capability, skills gaps, and opportunities for professional development and targeted training and seminars can be used to increase data skills and competencies. There are a range of organisations able to develop skills and competencies to uplift the data literacy across the workforce, including academia (universities and TAFE), a range of registered training organisations and the Australian Institute of Company Directors.

Creating communities of practice and encouraging professional development that has industry or professional recognition and qualifications across the workforce is also important.

ACS is a professional accreditation organisation, responsible for accrediting University IT courses nationally, as well as skills, training and competency assessments of people seeking visas to work in Australia.

Importantly, the ACS can offer SA Government as a whole, or individual agencies within the government, the ability to make use of the Skills Framework for the Information Age (SFIA) framework to assess skills alignment and certification of the workforce. SFIA is used to evaluate the necessary skills capability, assess development needs, and provide professionally recognised certification and qualifications for staff working in data and information, and a range of associated information-based activities.