THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

The University of Queensland's submission to the National Data Security Action Plan discussion paper

10 June 2022

This submission to the National Data Security Plan discussion paper compiles feedback from academic and professional staff from The University of Queensland, and includes UQ Cyber, ARC Industry Transformation Training Centre for Information Resilience (CIRES), UQ AI Collaboratory, School of Information Technology and Electrical Engineering, UQ Law School, AusCERT, UQ CSOC, UQ Information Technology Services division (ITS) and UQ Office of the Vice Chancellor.

A summary of our recommendations is provided below. Our detailed analysis of the four areas where the discussion paper calls for views, and context for each of the recommendations is provided in the remaining document.

- **Recommendation 1:** Form a national expert body to provide sector specific advice and guidance for data security
- **Recommendation 2:** Expert consultation on policies and regulations relating to research data sharing
- **Recommendation 3:** Develop data localisation approaches based on data type not organisation type
- **Recommendation 4:** Initiate a national effort into developing a shared understanding of data and security classifications
- **Recommendation 5:** Businesses of all sizes should have a minimum required level of data security
- **Recommendation 6:** Increase investment in education and training in data security at all levels
- **Recommendation 7:** Public campaigns to raise public awareness on risks of data security and misinformation

International Obligations

1. What do you consider are some of the international barriers to data security uplift?
2. How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?
3. What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?
4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market? a. What obligations are you most commonly subjected to from international jurisdictions?
5. Does Australia need an explicit approach to data localisation?

We note a number of barriers to Australia's data security uplift, which include **a lack of harmonisation and mapping of the data security legislation and expectations across different countries.** The fragmentation with different levels of restrictions (international as well as between federal, states, local governments) introduces a large number of challenges for data security. Markets and companies in different states treat data differently due to the different regulations in those states which have different levels of restrictions or different standards/rules. **Lack of literacy, knowledge and awareness of domestic and international laws and cross-boundary expectations** is a significant issue. Not all individuals and businesses are aware of domestic and international data privacy and security laws, how these affect them and how best to work within these boundaries. There is clear evidence of a general lack of understanding and awareness, when it comes to appropriate data use and sharing, both legally and ethically. For example, we have observed that large volumes of data are retained purely because the requirements are not understood and are therefore increasing their exposure to risks. These challenges exist internally but become greater when sharing data with (overseas) collaborators/third parties external to the organisation.

As a consequence, Australian businesses that are less resourced may choose to forego entry into the export market of a jurisdiction that has a more restrictive data security framework than that in which they are currently operating in. This presents a **barrier to entry into the new market**, and hence, reduces incentives to align or operate internationally. On the other hand, the alignment of Australia's framework to international data protection and security frameworks may mean that, in order to be able to be aligned to all frameworks, the most restrictive of controls from the collection of frameworks available are inadvertently adopted for all Australian businesses. For example, the most restrictive parts of General Data Protection Regulation (GDPR) would then have to be imposed on businesses in Australia. While some aspects of GDPR are positive and should be adopted (e.g., data portability principles), applying the entire GDPR in the Australian context needs further consideration. The enforcement load with adopting something along the scale of GDPR could be an issue as the adoption scales up. There are known difficulties for the EU to enforce the GDPR in a scalable way, which need to be considered into the planned Australian Government guidance, to avoid creating significant **barriers to innovation and technology advancement**.

There are opportunities for a federal government framework which is in line with international expectations, and at the same time homogenises across states and territories. We welcome the steps towards whole-of-government guidance on how best to align a business's data storage and transmission to the pertinent extra jurisdictional framework that each Australian business is venturing into.

Recommendation 1: We recommend the formation of a national expert body to provide sector specific advice and guidance for data security. Such a national, single go-to place, if adequately resourced, would assist in providing much needed support. For small businesses (e.g. sole proprietors) or individuals, a national expert body which provides guidance and resources on best practice would accelerate principles-informed approaches to data security. The principles could be promoted through succinct and effective messaging (e.g. commercials, campaigns). Additionally, a 'mapping' between prominent overseas legislations to domestic legislations would be beneficial. The government could consider developing some guidance on data handling and data sovereignty ratings, including which regions best align with Australian principles (e.g. https://ppl.app.uq.edu.au/content/6.40.03-data-handling). A standard approach to 'Data Sharing Agreements' could be helpful.

Data laws are constantly changing and being updated internationally, and it would help Australian organisations if the Australian Government could leverage the DFAT and Austrade offices to provide regular updates on data law changes to Australian businesses (via a dedicated team to translate and provide support to SMEs). Consulate services and DFAT staff could look at the local legislations of the countries they are stationed in, and then update these changes back to the authorised federal agency in Australia to consolidate this information. The local team in Australia from the federal government can then translate this into SME-understandable guides or matrices which they can refer to.

The Australian Government could also consider leveraging or encouraging multinational companies to support or automate such data framework alignments. Companies such as Google or Amazon facilitate the transfer of data across national borders and would be in a strong position to facilitate better compliance to international data protection and security principles. For example, the automation could consider data type and data size, or improve the situational awareness of data breaches or mishandling of data.

Adequate resourcing of such a body is critical. We note the challenges faced by some of the previous national expert bodies, such as growth centres.

Recommendation 2: We refer specifically to research data security, legislative and policy expectations, and advocate that research data sharing controls be carefully balanced with advancement of science, Australia's standing and position therein, and fostering of international collaborations within the scientific and academic community. This includes support for open access and data release for public good.

We recommend that academic experts on research data management are consulted and incorporated into the committees that inform policies and regulations for research data sharing and security.

Recommendation 3: Australia needs an explicit approach to data localisation. This must be done transparently (so that data owners are aware of where their data is being stored and how it is being used), to allow stakeholders to keep track of who stores sensitive data. At the time of writing, the current guidance is high-level and could be misinterpreted. We believe that the application of data localisation is tied to the type of data. There is a need to recognise the sensitivity of the data according to its type first before implementing localisation. The current focus is on the organisation type or the type of entity handling the data. For example, hospital data collected at a Queensland Health hospital currently needs to be localised. However, data from a private hospital in Queensland, which is operating as a business and not a government agency, may not need to be localised. This difference would result in the potential risk of exporting sensitive data overseas. If one only considers the nature/type of data, rather than the entity that produces/owns/collects the data, the data localisation approach would be more effective.

To implement effective data localisation approaches, we recommend increased investment in the research and development of new methods for federated learning, provenance tracking, and on-device computing which would support development of sovereign capability in these advanced areas.

Government's Role

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?

7. Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?

8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

One of the first steps towards better harmonisation across all jurisdictions is to ensure that the information/data security classifications are consistent across Australian Federal, State, and Territory governments. Currently, definitions and classifications across industry and states may be different to those used by the Federal Government. For example, 'Protected' in the government may differ from a classification used in business or within an educational institution.

Additional challenges include the different data classification across Government and other organisations on storage, transmission, time of storage, etc. There is no consistent data security practice across all levels of government. Currently, data sharing between organisations (across states) is challenging as information security classifications are not aligned with standards, and security controls could vary.

We expect that the federal government is ultimately responsible for ensuring consistent definitions, terminologies, vocabulary, and the clarification of processes. For example, the classification framework would fall under the Office of the Australian Information Commissioner (OAIC) and Australia Attorney General's department (e.g. currently the Protective Security Policy Framework (PSPF)). We acknowledge that enforcement has several challenges under multiple layers of governance. As such, the responsibilities and processes for enforcement need to be clearly assigned and clarified.

Recommendation 4: A national language/classification would help to reduce the confusion or the need to translate. Requiring a uniform standard across all of Australia harmonises the understanding of the levels of sensitivity and hence can catalyse policy alignments. This challenge becomes greater when looking abroad. Opportunities to adopt an internationally recognised classification framework could be helpful. We suggest the federal government to consider the lessons learned and the mechanisms used by the US Government in implementing, modernising, and enforcing the Federal Information Security Modernization Act (FISMA).

We recommend that a national effort is initiated to develop a shared understanding of data and security classifications. This shared understanding is a precursor to responses to the questions being posed in the paper.

Clarity and Empowerment for Business

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?

10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?

11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).

13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

There is extant literature available on the value creation from data, as well as ongoing work from both the Australian and international research communities on the various facets of data value (see e.g. cires.org.au and cyber.uq.edu.au). We also point out that an uplift of data security posture for businesses is less a function of their size and more of the type of data they create, share and consume. Levels of data security should therefore be based on the level of sensitivity of the data being collected, rather than business size. We further note that size of the business may impact on the capacity and resourcing available to the business for enforcement of data security protocols and best practice. Therefore, there may be businesses that are small, but actually hold sensitive information, which must transact the information across jurisdictions. Overall guidance is welcome (see recommendation 1), but it is important to acknowledge that small business in particular may not be in a financial or risk position that easily allows the implementation of overarching guidance.

Recommendation 5: Businesses of all sizes should have a minimum required level of data security. A mechanism for assistance and implementation of overarching guidance through a national expert body is desirable. Businesses that fall under the three million turnover threshold but are collecting sensitive information may operate in a manner that accepts data breach as an operational risk. These relatively smaller entities (e.g. not-for-profits helping disadvantaged children), should be provided with assistive repercussions instead of punitive actions, when following up on data handling complaints or actual breaches. This includes providing awareness of the data security obligations and guidance relevant to their business-as-usual activities. Particular attention may be needed to increase awareness and know-how data owners using third party technologies (e.g. cloud storage) to enable them to have better control and understanding of what goes on with their data.

With appropriate support, the government may consider mandatory data security licences to manage certain types of data, paired with enhanced accountability mechanisms for government agencies and industry in the event of data breaches. Such accountability should be well defined, e.g., who is accountable for what type of information.

Recommendation 6: We highlight the pivotal role of education on data and security and recommend that there needs to be a comprehensive coverage and levels of skills/responsibilities. For example, all undergraduate level programs should include a basic/universal course on data management and data security. There should be increased executive education, for example at board level (via MBA programmes across universities, and organisations such as the AICD). More importantly, high schools'

curricula should add data management and data security into the digital curriculum which currently focuses on coding and design.

Lack of skills and workforce shortages for skilled data and security personnel are significant. To promote 'sufficient awareness', we recommend investment in supporting the upskilling/reskilling to lift the workforce capability in terms of awareness/know-how of data security obligations. We propose for an increase in more Commonwealth supported places for study programs related to data and security.

Empowering and Educating Citizens and Consumers

14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

We observe that despite availability of accessible high-quality information, there are barriers to the discovery of that information by citizens and consumers (e.g. knowing about the Australian Cyber Security Centre (ACSC) website and finding relevant information on the ACSC website). As a result, there is an ongoing vulnerability and risk of data security within the community. The risk is not just in breaches of data stored by private companies or public organisations. The risk is also in data being manipulated and presented in ways that may be misleading and sending the wrong information, thus affecting decision making in a negative way. The focus should also be on ethical use of data not just avoiding leaks from private and public sector organisations.

Recommendation 7: The public information has to be 'out there', e.g. on television, public transport, billboards. There needs to be more effective public messaging (e.g. campaigns likened to anti-drink-driving commercials). To avoid being alarmist, national data security educational programs are needed (see previous section). Additionally, further active ways (e.g. workshops at public libraries) are also needed to increase data security literacy levels in the general public.

Contributors from UQ

- Prof Ryan Ko, UQ Cyber & School of ITEE
- Prof Shazia Sadiq, ARC Industry Training Centre for Information Resilience CIRES & School of ITEE
- Assoc Prof Gianluca Demartini, School of ITEE
- Assoc Prof Guido Zuccon, School of ITEE
- Geoffroy Thonon, UQ ITS & AusCERT
- Sasenka Abeysooriya, UQ Information Technology Services
- Marc Blum, UQ Information Technology Services
- Amanda-Jane Turner, UQ Information Technology Services
- Dr David Stockdale, UQ Information Technology Services & AusCERT
- Dr Andelka Philips, UQ Cyber & UQ Law School
- Shunyao Wang, UQ Cyber & School of ITEE
- Kate Aldridge, ARC CIRES & School of ITEE
- Kana Smith, UQ Cyber & School of ITEE

Contact details

uq.edu.au

cyber.uq.edu.au

cires.org.au

auscert.org.au

CRICOS Provider Number 00025B