



Australia's National
Science Agency

National Data Security Action Plan discussion paper

Department of Home Affairs

CSIRO Submission 22/794

June 2022

Main Submission Author(s): Surya Nepal

Enquiries should be addressed to:

Elizabeth Yuncken

CSIRO Government Relations

GPO Box 1700 Canberra 2601

T 02 6218 3547

E mplo@csiro.au

Introduction **2**

CSIRO response to selected questions in the Discussion Paper **3**

References **15**

Introduction

CSIRO welcomes the opportunity to provide comment on the Department of Home Affairs National Data Security Action Plan discussion paper. CSIRO is Australia's national science agency and one of the largest research organisations in the world. CSIRO's role within the innovation ecosystem is to solve the greatest industrial challenges through applied and innovative science and technology. As part of our work, CSIRO develops open code and technologically neutral solutions, which has allowed it to position as a natural trusted advisor for industry and government.

CSIRO contributes to building trust and confidence in Australia's digital economy and critical infrastructure through mission-driven cyber security research in areas such as the Internet of Things (IoT) security, human-centred security, Artificial Intelligence (AI) security, post-quantum cyber security, and information security and privacy. CSIRO is responsible for operating research infrastructure in a high security environment to deliver outcomes across multiple sectors within Australia and overseas, including government, research institutions, commercial and other non-government sectors.

CSIRO supports the strengthening of data security regulations to promote a growing digital economy and recognises the importance of the ongoing reforms required to outpace the complex threat environment. This submission addresses selected questions in the discussion paper that relate to CSIRO's scientific and technological expertise (Q2 and Q15 are not addressed).

CSIRO welcomes the opportunity to discuss these matters in more depth with the Department of Home Affairs. Please see the contact details on the cover page.

CSIRO response to selected questions in the Discussion Paper

1. What do you consider are some of the international barriers to data security uplift?

Based on our research and interactions with industry, CSIRO has identified the following barriers to data security uplift – these have been classified into two broad categories: legislative and technical. Each barrier is briefly explored below.

Legislative:

- A **lack of common legal frameworks and policies** on data storage and processing, despite the existence of strong international data sharing communities driven by national security (e.g. Five Eyes intelligence alliance).
- A **lack of interoperability between national legislations**; for example, how Australian legislation interacts with the European Union's General Data Protection Regulation (GDPR) and other frameworks.
- A **lack of common understanding** between legislation across nations; for example, different definitions of similar terms can make it difficult to understand, apply, and adapt international legislations and guidelines into the Australian context.
- **Absence of common international data protection and security frameworks** that integrate with the legal systems of the partnering countries.

Technical:

- **Incompatible technical (cryptographic, access control) standards** between countries may encourage convenience of data exchange by sacrificing data security.
- The **internet is not designed to control data** but operates on the free movement of data. Even the recent advancement in computation, communication technologies have an underlying assumption of free movement of large scale of data, e.g., 5G/6G. This means new overlay methods¹ are required to control the movement of the data.
- Countries that protect data by localisation methods may **fail to control data mobility** as trained Machine Learning (ML) / Natural Language Processing (NLP) models are often not considered in data movement. Consideration should be given to broadening the definition of "data" to include the artifacts of emerging critical technologies, more specifically Artificial Intelligence (AI) / ML. It has been demonstrated that in many cases, original training data can be inferred from those models [6, 7].

¹ Overlay methods are control methods, tools, and guidelines globally enforced (legally and cryptographically) in all jurisdictions where data can travel. It may mean local legislation aligning with globally accepted legal frameworks, e.g., GDPR.

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?

CSIRO has no views on this as an end-user, but we consider the following aspects to be critical to assist industry to meet a principles-informed approach to data security: guidelines tailored for end-user groups; easily accessible assistance; community involvement in guidance development; case consideration in international data related regulations; new funding models and incentivisation packages; and data security as a strategic business and risk consideration. These aspects are briefly explored below.

- **Guidelines tailored for end-user groups** (for example the CDR,) would greatly assist in meeting a principles-informed approach to data security. Specifically, we suggest that a community-driven approach be followed to develop such guidelines, to ensure that guidelines meet the needs, expectations, and skill level of the intended user groups.
- **Easily accessible assistance** is required to meet the principles-informed approach to data security and make the approach easier to follow at lower cost. This links closely with the requirement for end-user tailored guidance. Specifically, a co-designed approach to data sharing awareness campaigns aimed at specific end-user groups can be implemented to support the need for maturity. These might be co-designed with industry to ensure widespread industry uptake.
- Existing Australian data bodies are evolving into complex structures and therefore **community involvement** is key in preparing guiding documents that will align with and fit into these structures. Similar approaches have been undertaken by the Therapeutic Goods Administration (TGA) in the development of its cyber security guidelines, as well as other entities, such as the CDR, etc.
- **International data related regulations are best considered on a case by case basis.** While it makes sense to preserve data locality, supporting economic growth may require international data treaties using a reference framework such as the GDPR. There is no 'one rule fits all' in this, and therefore cases should be considered individually to best determine the recommended approach.
- **New funding models and incentivisation packages** can be established to support the digital maturity uplift. Future approaches must be driven by effective policy making, to align possible initiatives and strategies that could be adopted to effect nation-wide digital maturity uplift.
- **Data security should be elevated as a strategic business and risk consideration.** A top-down guidance on this would assist in raising the importance of data sharing and elevating the national consideration of data sharing and privacy perceptions on a national level.

4 a. What obligations are you most commonly subjected to from international jurisdictions?

CSIRO has carefully assessed and procured cloud services for the storage and processing of our selected research data. The protection of these outsourced data on international cloud service providers is key to our successful operation. Of particular concern is whether sensitive data is held, stored, and processed with free cloud service platforms enforcing no responsibility disclaimers (also refer to our comments to Question 5).

5. Does Australia need an explicit approach to data localisation?

CSIRO recommends that Australia needs an explicit approach to data localisation. The following reasons are paramount in our consideration of this:

- The "data storage and processing sector" is defined as a critical infrastructure sector in Australia's recently established critical infrastructure legislation. Hence, it is critical that sensitive data is stored and processed within the Australian jurisdiction.
- Business data of our Small and Medium Enterprises (SMEs) contains both IP and business intelligence. Considering the contributions that SMEs make to our national economy, it is important that business data resides and is processed within Australian jurisdictions.
- Individual citizens' data is important for both individual privacy and national security. Recent data breaches in Australia have highlighted how an individual's personal data has implications for national security. The incursion into the ANU and Toll Group are just two such examples of breaches with major downstream effects that are still being realised.

If data localisation is not applied, the following risks need to be considered:

- Australia and the Australian data owners do not have concrete control over who can access the data, how its accessed and backed up, or have any certainty of how many copies of a data file exist.
- The international company providing data storage and processing services is required to conform to the local regulations and legislation on data (where the service is located), regardless of the service level agreement the company has with their Australian client. Whilst the existing local regulations may be appropriate on the day the data is provided, changes will happen over time that may change the risk posture for that data. Further, mutual access arrangements between the Australian data owner and their collaborators, can lead to other parties in the jurisdiction of the collaborator having the ability to request and obtain access to data in their jurisdiction.
- The service providers may operate in a country such as Australia but store/back up the data in a data centre located in a different country. It is difficult to track and reconcile Australian data security policies with respect to different countries and there is no national, Australian legislation or regulation to enforce this standard. Further, data security and privacy policies are evolving.

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?

Consider an example of the energy sector. Many regulations governing energy data security, access and sharing are at the state jurisdiction level which can make the development of uniform and scalable national approaches challenging. Energy data sharing is currently restricted owing to a range of commercial, privacy and confidentiality risks. However, there are also clear risks of not sharing data in reduced energy affordability, reliability, and sustainability. The Energy Security Board Data Strategy and the Consumer Data Right for Energy outline critical regulatory changes toward facilitating improved energy data access while protecting consumer privacy and confidentiality.

CSIRO suggests a data security policy and framework be considered at a national level. One way of achieving better harmonisation is by establishing a committee / task force across all jurisdictions to ensure consistency in terms of locally applied data security policies. This could contribute to addressing some of the legal barriers identified in the response to Question 1 (albeit on a local level), to ensure:

- Coherence on a local level in terms of a national common legal framework and policies on data storage and processing.
- Inter-operability between local jurisdictions in the context of data security.
- A common understanding between local jurisdictions considering relevant terms and definitions.

Not all jurisdictions are at the same maturity level of data security. By putting in place such an intra-jurisdictional committee / task force, the more mature entities could lead the way in establishing good practices based on international policies and frameworks. The less mature jurisdictions would be able to increase their maturity exponentially faster as they will have local counterparts to learn and adapt from. By working together in this way, Australia can develop a single and united front in terms of data security, facilitating better communication, smoother data transfer and safer data storage, and supporting Australia to establish legislation, processes, guidelines and a compatible and aligned policy framework.

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?

While some attempts to coordinate data security in local government settings have been made through all Premiers' offices, we observe limited coordination between the state governments and Australian Government. In CSIRO's view, data security policy and framework is best led at the

national level with the implementation of such a framework part of general cyber security management scheme in all agencies and organisations and at all levels of government.

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?

Based on our discussions with industry partners, the main barriers facing industry as a result of inconsistent data security practices are the cost of data collection, management and communication of data, distribution of the benefits from data and the loss of competitive advantage. Also, the management and handling of data, particularly data related to private and confidential aspects of commerce, is not universally regulated. Therefore, data sharing and the associated privacy aspects thereof can be viewed differently, with varying levels of distrust. Privacy preserving algorithms such as data anonymisation, obfuscation, cryptography, and access control mechanisms to protect privacy and confidentiality of data, have been proposed and widely accepted in academia. However, the acceptance of sharing data using these techniques depends on the knowledge and perception among the end users. It is necessary to understand how all businesses develop their data security perceptions to effectively provide correct information and eliminate misinformation.

Despite numerous advances in data sharing initiatives and privacy preservations, many studies still find significant barriers for sharing and reusing data [8]. Of these barriers, the perceived risk of sharing and reusing data remains one of the most prominent concerns. Generally, limited and restricted access to data, impacts not only products and services, but also the competitiveness of Australian owned and operated businesses. For example, Australian government and state government agencies control most valuable data which SMEs do not have a mandate or cannot afford to collect and maintain, which can impact on the competitiveness of these organisations. In addition, data is managed with different systems and platforms. Security practices can vary significantly between these different contexts, making it difficult to compare actual security protections, share security practices and knowledge, and comply with security requirements.

Government agencies collect and produce large amounts of data that is not utilised further outside of agencies' core operations because the agency is the only entity authorised to collect and use such data. Similarly, in business, each organisation collects its dataset from its clients, and sharing these datasets is often challenged by IP, privacy, ethics, and business confidentiality concerns. The low utilisation of data across governments and businesses can result in an impediment to data-driven innovations. Many government agencies have difficulty finding specialised solutions in their core operations. For example, collecting and maintaining child abuse materials (e.g., pictures and videos) is naturally illegal, and this also prevents the development of advanced specialised tools to help law enforcement agencies. It is often infeasible for an agency to employ the required specialists to innovate, develop and maintain such specialized tools. For example, a company sells its products to many agencies worldwide, while an agency needs to bear the entire cost alone for one use case. Maintenance at the professional-grade is key as technology evolves and products become obsolete quickly. Moreover, companies and research organisations are better suited to attract such specialists.

In CSIRO's experience in the energy sector, a greater level of controlled data sharing, while maintaining privacy and security, could help to secure a reliable, affordable, and fair transition to a net zero emissions future. The future decarbonised energy system will require consistent, actionable data to ensure efficient system operations, avoid capital overbuild and secure fairness for all Australian energy users, not least vulnerable groups in society.

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?

The value of data can vary depending on its use, research purposes, commercialisation, or sensitivity. CSIRO collects, receives and generates data for its internally and externally supported projects. Such data is retained for a period of time, depending on its value and the specifications / expectations of the project. The data security obligations are project driven often by the individual contract terms with a client (e.g., the client supplying data may require it to be disposed of after the delivery of the project) or ethics approval (e.g., data collection approved with the condition that data is disposed after the project). In some cases, there will be limitations on data usage beyond the project duration. A national framework on data security could help to harmonise the data security requirements and increase the utilisation of data.

There are a number of steps that could be taken to better support businesses to understand, appreciate and manage their data value:

- In CSIRO's experience, businesses often **do not understand that all data are not equal in value**. To a lesser extent, businesses lack an understanding of the value of data to individuals and other stakeholders. What is often seen as low value by the collecting businesses may have greater value for other stakeholders (or data owners). This puts an enormous burden on businesses as they are dedicating significant resources to protect all data. To address this overcompensation, it is important that businesses understand the value of the data they have. Currently, Australia does not have a framework to classify data in terms of value and contribution. A simple guideline or criteria to identify and classify the value of the data while applying data security principles could be very helpful.
- In CSIRO's experience, **businesses often do not have sufficient awareness of their data security obligations**. Although there is some guidance available to support awareness of this aspect, the rate at which data is generated exceeds most entities' ability to manage the data and understand its full contribution and value. Specifically, awareness of data security obligations is very limited in certain sectors. Particularly, small sized enterprises are not aware of their data security obligations and guidance could be customised to support them in a way that would not add to their administrative load. Medium to large sized enterprises often have a mature information security management program and understand their data security obligations. As can be seen by the Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report 2020-21, medium sized business reported the greatest average financial loss from cybercrime activity.
- **Cloud storage services are used to store sensitive and critical data**. Although there are guidelines available to support the use of cloud storage, there is a lack of a standard

authoritative guideline for businesses to follow. A common standard guideline at the national level would be beneficial.

- **Businesses share models without realising that they are sharing data (stored in the model in numerical forms)** that can be used to generate original data. With the emergence of advanced AI/ML, data can be exchanged in a hidden form. For example, an ML model can learn more than necessary, and a badly designed model could potentially reveal the original data. To address this, the definition of the data needs to be extended to data stored in models, graphs, and software components in different formats.

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

CSIRO suggests the development of a single, cross-jurisdictional data storage and processing framework that conforms to all Australian and international requirements is critical to equip, support and uplift the Australian digital economy. It would level the playing field and support Australian business (CSIRO, other large, medium, and small entities alike) to compete on an international level, without having to spend undue time and resources to research and apply international data protection mechanisms of their own accord.

To assist businesses that find it difficult to balance its data utility with the need for security and privacy, the Australian Government could provide a clear guideline on comprehensive cyber security, covering data security.

CSIRO recommends that consideration also be given to the following to help businesses:

- **A simple, easy to understand guideline for implementing data security principles** (see response to Question 3). Enabling all Australian businesses to work from the same set of reference data security principles will make it easier to ascertain an accurate level of data security understanding, implementation, and compliance within Australia.
- **A framework for harmonisation of data security requirements across different jurisdictions** (see response to Question 6). A single source of Australian truth will make it easier for new entrants to the data security domain to understand and interpret relevant obligations.
- **A platform/avenue for sharing best practices among businesses** which could be facilitated through the cross-jurisdictional task force, where business can share their experiences and learn from others that are more data security mature than themselves (see response to Question 6).
- **A framework (in the form of a simple guideline or criteria document;** see response to Question 9) that can assist businesses in understanding the value of the data. This will support businesses to invest time and resources in protecting data that requires protection, and not spend unnecessary resources on protecting data that does not require as in-depth protection.
- **Tools and procedures to better utilise government data** (see response to Question 8). The Australian Government has a magnitude of data that reflects the Australian public. Making these datasets available to businesses in a responsible manner will facilitate better

collaboration between the government agencies and local businesses, and result in better service delivery from local businesses to the community.

- **Targeted awareness campaigns and tools** (see response to Question 9). In general, cyber and data security and privacy is considered as an add-on and is not built-in to business operations. Targeted guidance, through end-user focused guidance documents and practical support tools, can assist specific user groups in uplifting their digital maturity.

By putting these measures in place, the Australian Government will help all local businesses to uplift their cyber security capacity and data security, and support them in improving service delivery for their clients, enhance business reach to larger, potentially international clients, and provide a strong national capacity in terms of digital maturity of local businesses.

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?

CSIRO is one of the largest data organisations in Australia. We are the largest provider of open research data in Australia and our internal data holdings amount to over 200 petabytes under active management with hundreds of petabytes more in offline storage. Given the importance of data to the organisation our data storage infrastructure provides close to banking levels of resilience.

CSIRO research is diverse and brings some of the most diverse requirements for data management, storage, and security in a single organisation. The data in one science area is often very different to that of other science areas. For example, our science domains range from climate science, health and biosecurity, minerals and energy, agriculture and food, to space and astronomy. We are also the largest provider of national collaborative research facilities in Australia. CSIRO has implemented procedures for risk based decision making around science data and has established practices of handling data for high security requirements such as in Defence or national security related projects and even in other domains. CSIRO practices are well above best practice level.

The CSIRO Cyber resilience team, reporting to the Chief Information Security Officer, undertakes cyber risk assurance of suppliers in relation to their security practices to protect CSIRO information they may collect, store, process or transmit. These reviews cover enterprise IT suppliers and potential suppliers of IT services to science where these have been identified through project and enterprise level risk assessments.

The process is time consuming, resource intensive and likely replicated across government agencies. Many of these suppliers are common across government, but many are also specialist to CSIRO and the Australian research community. Visibility of cyber supplier assessments for whole of government procurement panel or standing offer participants would be a significant step forward. More cooperation across government in sharing risk assessments where they have been undertaken to support more bespoke procurements would also be very helpful. CSIRO recognises that this information would be 'In confidence' to government agencies and departments.

For the business sector, CSIRO suggests that there is an opportunity for government to support the development and promulgation of common guidelines, methods, and processes to identify and mitigate risks while working with commercial clients and international collaborators.

In previous research conducted by CSIRO [**Error! Reference source not found.**], we identified a number of barriers, both social and technical, that could introduce structural constraints in terms of the choice of decisions that supply chain participants can make. Specifically:

- We identified several benefits as well as barriers and risks of data sharing, but an **inconsistent view in terms of perceived benefits and risks**. We found that individual actors of the supply chain perceive little benefit compared to several perceived risks/disadvantages when they share data. As such, online sharing of data may be skewed to those sectors that are more open to online data sharing.
- **Asymmetry in the willingness of data sharing among upstream and downstream** of supply chain actors was apparent and in line with previous research. Although this is in part due to a result of privacy concerns, this relates to human nature – supply chain participants generally do not provide positive feedback, but they are more inclined to provide negative feedback (in the form of complaints).
- **Privacy and confidentiality are used ambiguously by different actors**. In the context of privacy law, the meaning of privacy is focused on data about individuals, whereas the term privacy is sometimes used to mean much more than the personal data, including information at the organisational level.
- **Trust and power were found to be important factors for data sharing**. Concerns were raised that others (competitors and non-competitors) could be reaping more benefits than themselves. Privacy preserving technologies are perceived as having a positive impact on people who see value in sharing data and who trust others with their data, but have concerns about organisational confidentiality and privacy. It was clear that the cost of infrastructure for data sharing and providing data sharing, need to be managed in a way to allow all actors to benefit. It was, however, apparent, that there is an overlap between the data that consumers would want to protect, with the type of data that organisations would want to protect.

From this we can deduce that perception of privacy is still a big holding point in terms of data sharing within the supply chain.

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?

In CSIRO's experience, size of a business, either in annual turnover, number of employees, or other traditional measures is a poor proxy for the amount or level of sensitivity of data that it collects, holds, and/or process. We do not consider this an adequate measure to guide data security as there are many examples of small businesses that deal with large volume of personal data and/or containing large amount of sensitive information. For example, the August 2020 data breach of

more than 50,000 NSW driver licenses was not attributed to the NSW government service delivery agency, but rather to a commercial entity [5].

The Discussion Paper for the Review of the Privacy Act (1988) [**Error! Reference source not found.**], released in 2021, presents a detailed argument on pages 44-48 describing the advantages and disadvantages of a size threshold for businesses to comply to the Act. While these points were made in the context of data privacy, most of them are readily relevant to the wider context of data security. It touches on the removal of the threshold, how to set it, what could be done to support small businesses to comply, how to simplify rules/guidelines depending on size, etc. Applying the rationale of this discussion paper to data security, security cannot be measured according to size, as the size of the business is not directly linked with data ingestion capacity. This is specifically relevant as cloud services are accessible by all SMEs, who might be excluded if a *size criteria* is adopted.

In CSIRO's view, it may be more appropriate to consider *data sensitivity as a criteria*. For example, an SME can be appointed as a designated contractor for the Defence domain, based on their skills and expertise. Due to the nature of their interactions with Defence and the direct or indirect role they would play in terms of national security, this sensitivity of data would be a much more appropriate measure.

Businesses do not consistently apply the data security principles used. It is thus important to provide overarching guidance on securing data, independent of the company's size. However, the Australian Government should give further consideration to providing assistance and support in the implementation of the guidance for small and medium-sized companies since they are less likely to have experts who can understand and implement the guidance correctly.

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

Some common factors CSIRO has identified through our work that are preventing Australian industry and businesses from developing and implementing an enhanced data security plan include:

- **Skills shortage:** Industry and businesses are suffering from skills shortages in cyber security and data privacy. Without the right people appointed with the right skills and knowledge at the right point in time, businesses do not have the capacity to effectively address any digital security aspects.
- **Priority:** Data security is not a high priority for industry and businesses. Unless the industry and businesses suffer from severe data breaches, the data security often does not get the attention it deserves. In addition, the focus of many organisations is firstly their core business, followed by physical security. Digital security is often applied ad hoc and only in response to incidents. For example, the revelation of the ANU data breach has forced the university sector to enhance its data management regime.
- **Drift:** Evolving legislation (e.g., critical infrastructure) and emerging technology (e.g., AI, Quantum) cause a constant drift in data security and privacy requirements. It is hard to keep

up with changing environments as the domain and its related regulations and security expectations are constantly evolving.

- **Usability:** Industry and businesses struggle to understand the obligated security requirements. It is hence important to provide the data security framework in a form that can be easily interpreted and implemented. Making assisting tools available would be beneficial for the industry and businesses. These tools should support humans in enabling cyber security, and where possible, include automation to remove some of the administrative burden currently on humans to maintain digital security.
- **Competitive advantage:** Businesses can lose their competitive advantage if they limit their services and solutions based on data security regime in scenarios where there is not enough technical support.
- **Jurisdictions even within the nation can be a blocking factor:** Data security regimes might be a priority for one state or agency and not yet high priority for others. Often there is no unity and clarification even within the same state. In most cases individual government agencies hold the responsibility to adapt a regime despite the above listed regimes. This can result in isolated gold valued data in government agencies. This is also due to a lack of guidelines and processes to support data custodians in government.
- **A lack of broader security awareness and literacy across the community:** for example, SME business owners are unlikely to have the security literacy needed. Even some CEOs struggle with basic security literacy. Consideration should be given to incorporating security awareness and literacy into education at all levels.

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?

In CSIRO's experience, Australia is behind Europe when considering the public awareness of data security and privacy.

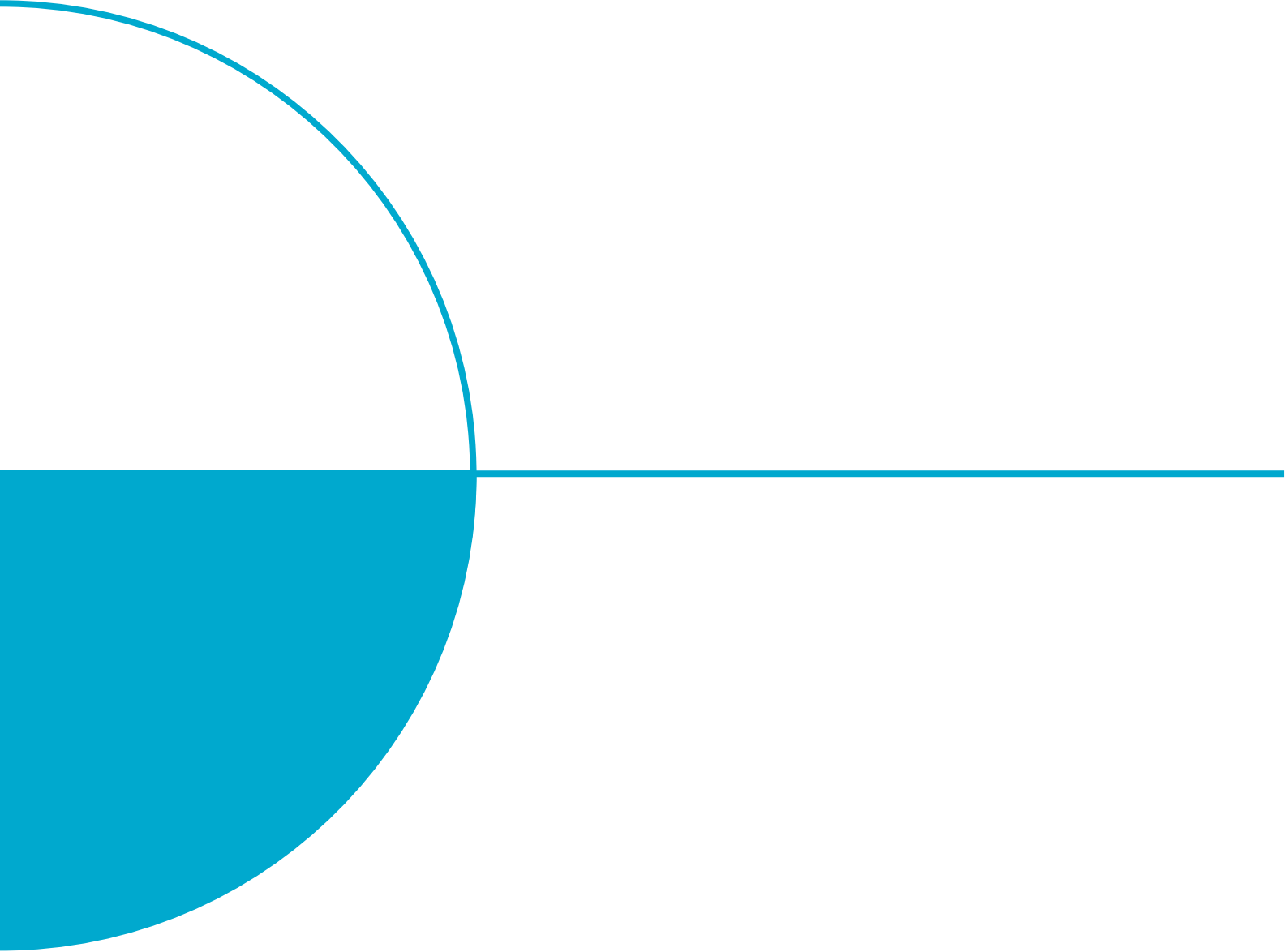
- Many guidelines exist related to cyber security, particularly focusing on securing IT assets, but very little guidance exists on data security. Currently, there is not a single source of information for citizens on the best practice for data security. A national agency such as the Australian Cyber Security Centre (ACSC) could produce usable guidelines for citizens and businesses and run regular workshops and information sessions on how to design and implement them as individuals and organisations. Such guidelines could be tailored to a range of communities: citizens, SMEs, larger enterprises, research organisations, government agencies, etc. Targeted guidelines with relevant examples on a usability scale could assist in educating both citizens and companies about the risks, perceptions, and benefits of casual data sharing.
- The boundary between personal data and public data is also blurred. There are a number of major difficulties in dealing with privacy perception in terms of data sharing, most pertinently the paradoxical use of users. Specifically, we witness what is known as the

privacy-paradox [**Error! Reference source not found.**], where citizens are trading personal information for short term benefits, feeling safe to provide information social media platforms, and companies mining such information to gain business intelligence. Advances in AI, more specifically ML and Natural Language Processing, have made it possible to analyse such public information to extract personal information such as age, sexual orientation and race of an individual that is considered sensitive. There is a need to develop security and privacy guidelines for citizens for emerging services and platforms like Internet banking, Facebook, LinkedIn, etc.

There is also lack of freely accessible tools and services to support end users. As per the response to Question 10, targeted guidance, through end-user focused guidance documents and practical support tools, can assist specific user groups in uplifting their digital maturity. This is relevant to both businesses and individuals, as the Australian Government has the mandate to ensure the safety of all Australians. For example, in the energy sector, additional information would be welcome to help consumers and citizens safely contribute data to energy affordability, reliability and sustainability in the transition to net zero while also protecting their privacy and confidentiality. This would be alongside clearer direction and guidance to government data custodians on the controlled release of energy data.

References

- [1] Anonymisation Decision Making Framework (ADF). ND. Available from: <https://ukanon.net/framework/> (Accessed 15 May 2022).
- [2] Data61. 2017. *A framework for data de-identification*. Available from: <https://data61.csiro.au/en/Our-Research/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework> (Accessed 15 May 2022).
- [3] Attorney-General's Department, Australian Government. 2020. *Review of the Privacy Act 1988 – Terms of Reference*. Available from: <https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-terms-reference> (Accessed 12 May 2022).
- [4] Alexander Krumpholz, Marthie Grobler, Raj Gaire, Claire Mason, Shanae Burns. 2021. *Raising Trust in the Food Supply Chain*. NDSS 2021. Available from: <https://www.ndss-symposium.org/ndss-paper/auto-draft-176/> (Accessed 12 May 2022).
- [5] Edward Pollitt. 2020. *54,000 NSW driver licences exposed in data breach*. Available from: <https://ia.acs.org.au/article/2020/54-000-driver-licences-exposed-in-data-breach.html> (Accessed 15 May 2022).
- [6] Congzheng Song, Thomas Ristenpart, Vitaly Shmatikov: Machine Learning Models that Remember Too Much. ACM CCS 2017, 587-601
<https://dl.acm.org/doi/10.1145/3133956.3134077> (Accessed 15 May 2022).
- [7] Congzheng Song, Vitaly Shmatikov. Overlearning Reveals Sensitive Attributes. ICLR 2020
<https://openreview.net/forum?id=SJeNz04tDS> (Accessed 15 May 2022).
- [8] Tenopir, Carol et al. "Data sharing, management, use, and reuse: Practices and perceptions of scientists worldwide." PloS one vol. 15,3 e0229003. 11 Mar. 2020,
[doi:10.1371/journal.pone.0229003](https://doi.org/10.1371/journal.pone.0229003)



As Australia's national science agency and innovation catalyst, CSIRO is solving the greatest challenges through innovative science and technology.

CSIRO. Unlocking a better future for everyone.

www.csiro.au