Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

1 August 2018

Dr Philip Green
Department of Prime Minister & Cabinet
1 National Circuit
Barton ACT 2600

NEW AUSTRALIAN GOVERNMENT DATA SHARING AND RELEASE LEGISLATION: AUSTRALIAN PRIVACY FOUNDATION RESPONSE TO ISSUES PAPER

This submission is made by the Australian Privacy Foundation, the nation's pre-eminent and independent civil society organisation concerned with privacy. Information about the Foundation is available at privacy.org.au.

The submission builds on comments made by Dr Bruce Baer Arnold (Foundation Vice-Chair) at the consultation meeting in July 2018. Foundation representatives would be pleased to meet with you in Canberra or Sydney regarding the issues discussed below.

The following pages respond to the Issues Paper generally before addressing specific questions in that Paper and highlighting concerns.

In particular, the Foundation considers that the proposed Purpose Tests are overly broad and will thus potentially be at odds with the respect for privacy as a core Australian value and a basis for public administration. Any erosion of privacy through data sharing must be proportionate rather than driven by bureaucratic convenience or unexamined claims by entities that are seeking to use data.

The Foundation considers that transparency regarding data sharing across the Commonwealth government and with non-government entities is both fundamental and consistent with the Government's commitment to accountability and process improvement through 'open government' initiatives. In essence, there is national benefit in seeing what is being shared, why it is being shared and how it is being shared. Costs associated with that transparency are a part of the social licence for the mandatory collection of data from Australian citizens/organisations and for the sharing of that data by government. In introducing a data sharing regime in the 'age of big data' and 'democratic deficit' it is necessary for government to reconceptualise itself as a data custodian rather a data owner, a servant of the people rather than a master.

Introduction

The establishment of a coherent and progressive data sharing regime at the national and state/territory levels has the potential to foster public engagement with government and assist national productivity.

The Foundation accordingly welcomes the willingness of the Department of Prime Minister & Cabinet to consult with civil society representatives and other stakeholders regarding the establishment of such a regime.

The consultation is of significance as both –

- an indication of the Government's commitment to accountability (addressing what has been characterised as a disquieting democratic deficit in Australian public policymaking and implementation) and as
- a mechanism that will potentially avert the substantive problems evident in current implementation of the national My Health Record (MyHR) scheme.

The Foundation endorses comments in the Issues Paper and in reports by the Productivity Commission and other bodies regarding the complexity and inconsistency of data sharing arrangements across the Australian Public Service (and by extension between the Commonwealth and other Australian jurisdictions), reflected more broadly in the absence of a principles-based whole-of-government approach to data collection, data processing and data sharing.

That architecture has resulted in a proliferation of agencies, statute law, regulations and administrative authorisations that inhibit efficient public administration, potentially erode accountability and substantively weaken the respect for privacy that is expected by all Australians.

It has been accompanied by a lack of transparency about what is being shared, why it is being shared, how it is being shared and how it is being processed. That opacity is not necessary and is contrary to community expectations regarding government accountability. It is not resolved by provisions in a range of statutes that provide for undisclosed sharing with for example 'any established regulatory body' and 'a body established by the Commonwealth'.

As the following paragraphs indicate, the Foundation – along with other civil society bodies – is supportive of improvements to the current information regime but cautions about measures that will increase rather than reduce complexity, that will inappropriately privilege particular interests and will substantively erode privacy protection. That erosion is of particular concern given the incapacity of the Office of the Australian Information Commission (OAIC), the deficiencies evident in legislation such as the *My Health Records Act 2012* (Cth) and misunderstanding among some data sharing proponents of the ease with which ostensibly de-identified personal information can be both re-identified and exploited in ways not envisaged by data custodians.

It coexists with concerns, evident in several high-profile overseas initiatives, that governments have failed to adequately price geospatial, health and other data that they have sought to market.

The Foundation therefore highlights the need for greater clarity regarding reference to 'new arrangements' to provide efficient, scalable and risk-based trusted data access to datasets that have substantial and community-wide benefits for research, innovation and policy

The emphasis in the Issues Paper on a principles-based approach and on 'five safes' is commendable. It is imperative that in developing the proposed legislation the Department should be mindful of problems with MyHR, where there is

- substantive disquiet among the health, legal and information technology sectors regarding defective system design and implementation,
- inadequate community consultation,
- evident uncertainty among administrators about salient aspects of the MyHR scheme

The Foundation notes that concerns regarding MyHR are not isolated. They are evident in recurrent criticism by the Australian National Audit Office of other major Commonwealth information technology initiatives and as noted by several members of the Foundation's Board are evident in overseas data sharing initiatives such as the UK care.data program.

Sharing personal and non-personal data is importantly not an end in itself. The Foundation emphasises the need for a strong understanding of risks. It emphasises the need for effective governance, with

- properly-resourced administrative oversight – something that goes beyond reference to agency-level 'champions' and the establishment of a Data Commissioner alongside the FOI and Privacy Commissioners
- meaningful engagement with civil society – something that includes both timely public education and a stronger presence on the Data Commission Advisory Council
- establishment of the Commissioner as an entity with the status of the Auditor-General or Independent National Security Legislation Monitor, reporting directly to Parliament on a timely basis

It also emphasises the need for transparency. The traditional axiom that sunlight is the best disinfectant – a disinfectant for misplaced fears, administrative malpractice, institutional over-reaching and disregard of substantive accountability – remains true. If sharing is to take place within and beyond Commonwealth entities that sharing must be disclosed in all other than exceptional circumstances. In essence, if you have a social licence to mandatorily acquire, process and share data you have a social responsibility to disclose on a clear, timely basis that you are doing so.

The Foundation notes the 2015 Australian Government Public Data Policy Statement. Policy statements lack teeth and are susceptible to misinterpretation or disregard. The proposed Data Sharing Bill must have a clear Objects provision that

- expressly enshrines privacy as a right (and that does not erode protection under the *Privacy Act 1988* (Cth), and
- represents a strong commitment by the Australian parliament to a regime in which privacy is respected rather than seen as a value that should be readily disregarded when an interest group makes claims about industry development, academic research or otherwise, and
- includes public disclosure of data sharing activity, and
- will be understood by all Commonwealth entities,

Understanding by agencies and the commitment noted above is salient because of practice over the past decade regarding information sharing under the Freedom of Information (FOI) regime, in essence a data sharing regime (and one that contrary to recurrent alarmism has not crippled public administration). People within and outside the Australian Public Service have for example been disquieted by recurrent statements from Public Service Commissioner John Lloyd that such access was "pernicious", "unnecessary" and "contrary" to effective public administration. Lloyd's statements are contrary to the express Objects in the FOI statute but are consistent with the reluctance of many agencies to give effect to the statute.

The benefits of data sharing that are identified in the Issues Paper will **not** be achieved unless there is substantive commitment on the part of the Government, there is 'buy in' by Opposition parties and the proposed regime strongly respects privacy through for example effective management of risk. It is imperative that the Government in establishing a future-proof risk management regime take on board the very substantial body of research on re-identification, acknowledge incidents such as the recent major data breach of Singapore's MyHR-style national e-health system, and critically evaluate claims

from solution vendors and bodies such as the Digital Transformation Agency whose culture/skills embody a dot-com 'get it out and then fix' philosophy that is inconsistent with public accountability.

The Foundation notes the Productivity Commission's acknowledgement in its 2017 *Data Availability and Use* report of a "lack of trust by both data custodians and users in existing data access processes and protections" and the Commission's emphasis on value, choice, transparency and confidence, in particular proactive management of risks. That confidence will not be forthcoming is the data sharing legislation is inappropriately permissive and if existing problems with the OAIC are perpetuated. In moving forward with development of the Bill the Department would usefully engage with civil society about the *Privacy Act 1988* (Cth).

Rather than establishing the Data Commissioner alongside the FOI and Privacy Commissioners it would be useful to consider the data sharing Bill as an opportunity for:

- taking on board the recommendations of the Australian Law Reform Commission and parliamentary committees about enhanced respect for privacy
- updating the *Privacy Act 1988* (Cth) to reflect the emerging environment of 'big data'
- revivifying the culture and resources of the OAIC, including providing it with the requisite technical expertise and addressing substantive concerns regarding regulatory capture
- developments in benchmark nations, for example Canada's current major revamp of its 1982 Access to Information Act and the EU General Data Protection Regulation.
- reflecting the FOI principles by meaningful disclosure of data sharing practice
- enacting human rights legislation to ensure basic human rights for all Australians

The DS&R Bill

The Foundation endorses the development of principles-based that expressly acknowledges privacy as a right and as a value that must be respected by all Commonwealth entities. That respect is not antithetical to sharing (within and outside the public sector) of personal information.

The Foundation strongly encourages the Department to consult widely and deeply, on a timely basis, about the interaction of the Bill with existing information and rights legislation, in particular the *Privacy Act 1988* (Cth).

In considering the express Objectives of the proposed legislation the Foundation – in noting reference to 'Commonwealth entities and Commonwealth companies and include most data collected by these entities' – considers that the legitimacy of data sharing will be reinforced by characterising those entities as curators (custodians) of data that respect Australians in acting in the national interest. It is desirable for agencies to move beyond their unstated sense that they are data owners who can pursue institutional benefits by sharing with other entities on the basis of bureaucratic convenience and/or where there has been an assertion that sharing will assist research, law enforcement and industry development. Ultimately much information held by government has a mandatory basis: people have no choice in provision of personal and other data. 'Sharing' should recognise that basis and should be disclosed.

The Foundation as indicated at the July consultation is not opposed to sharing per se. One reason for contextualising the proposed Bill in relation to the current FOI regime is that sharing may indeed result in greater transparency around government activities and spending. In that sense sharing is justified as a mechanism for enhancing trust in public administration.

Principles

The Foundation notes reference on page 8 of the Issues Paper to safeguards and trust. Specific reference to respect for privacy must be 'at the core of the new legislation' if safeguards and trust are to be meaningful. Trust will be fostered by disclosure of data sharing activity, discussed in more detail later in this submission.

The Bill must provide for credible enforcement powers. The Foundation notes advice from the Department that the Data Commissioner will have a staff of around 18 people and will be able to draw on technical support from the Australian Bureau of Statistics.

As indicated above, the Foundation considers that the Commissioner needs to have an independent status, reporting directly to the Australian Parliament and being in a position to build trust by criticising agencies and ministers where the principles have been disregarded. In essence, the Commissioner must have teeth – something achievable through statute – and be prepared to use them. Regrettably that has not been the case with the OAIC and it is unsurprising that some stakeholders have expressed the view that the OAIC should be reformed.

The Foundation acknowledges the proposed establishment of an Advisory Council to advise the Data Commissioner. Drawing on study of existing Advisory Councils the Foundation considers that the Council should provide Parliament with an independent annual report (the cost is appropriate as a base for good governance and trust) and should be sufficiently resourced for effective oversight rather than simply providing expertise on a non-commercial basis.

As importantly, the Council should be truly inclusive. Membership should not be weighted to research and commercial interests; it should instead clearly encompass the range of civil society perspectives if data sharing is to gain acceptance as legitimate.

The following paragraphs, in addressing specific questions in the Issues Paper, will be useful in informing official and community discussion about the proposed data sharing regime.

1 Are these the correct factors to taken into account and to guide the legislative development?

The Foundation notes the fundamental significance of express reference in the legislation to privacy, in particular as part of Objects provisions. Respect for privacy must be articulated as one base of the proposed Act rather than as an inconvenient impediment to the sharing of personal data within the public sector or the provision of data to non-Commonwealth agencies.

In moving ahead, the Foundation urges the Department to provide a detailed Privacy Impact Assessment, consistent with the stated commitment to Open Government. It urges the Government to provide the requisite period for meaningful public consideration of the Exposure Draft Bill rather than aiming to fast-track the exposure process at the end of the year. Data sharing has significant public benefits but the legislative framework must be correct: in essence a 'get it right the first time' and then enhance on an ongoing timely basis approach rather than 'policy by media release' approach is suggested.

Recommendations:

1.The objects must include a specific reference to privacy

2.A Privacy Impact Assessment must be conducted by an independent body

2 What else should the Government take into consideration when designing the legislation?

As far as the Foundation is aware there has not been a coherent overview of the 'different types of data held by government', the extent to which sharing within government is sought by agencies and the rationale for that sharing, and the likely interest in the private sector. In situating the proposed legislation within accountability and open government philosophies it would be useful for the Department to provide such an overview, either through its own resources or through assisting a national workshop. Civil society organisations, lawyers and others have for example indicatively mapped intra-government sharing in particular sectors. Trust would be fostered by greater transparency about what is currently shared and what agencies want to share in future.

The Issues paper identifies authorised sharing for 'particular purposes only'. The purposes identified in the Paper are very broad. They include 'informing government policy making', 'supporting the efficient delivery of government services or government operations', 'assisting in the implementation and assessment of government policy' and 'research and development with clear and direct public benefits'. Such a charter must be bounded by respect for privacy that is given effect through administrative protocols that are more forward-looking than the guidelines used by the OAIC in interpreting the Australian Privacy Principles in terms of 'reasonableness' as lowest common denominator practice.

The Foundation notes reference to 'accredited bodies' subject to built-in accountability under the proposed legislation. As indicated above, the Data Commissioner will need both meaningful enforcement powers and a willingness to use those powers, along with expertise that prevents regulatory captures by government agencies and data end-users.

Civil society remains unclear about the interaction of the Data Commissioner and the OAIC. The Foundation considers that the proliferation of information agencies is undesirable: a balkanisation of responsibilities and spreading of resources tends to foster regulatory arbitrage, will result in confusion and will erode trust.

The Foundation considers that disclosure of data sharing is an appropriate accompaniment of the social licence to share. In essence, Commonwealth entities should disclose on a timely and readily accessible basis what they are sharing, why and how. That disclosure might take the form of a 'disclosure statement' on websites and in annual reports. It is not contrary to sharing; instead it provides accountability and reflects the goods that were identified by the Productivity Commission. It is not synonymous with requirement for meaningful consent by specific individuals to whom the data relates.

For any personal information, meaningful consent is required to do anything with that information. According to the OAIC the four key elements of consent are that the individual is adequately informed, the consent is given voluntarily, the consent is current and specific and the individual has the capacity to understand and communicate their consent. Consent must be not bundled. Privacy is about the control of personal information. It is a fundamental human right to be able to control personal information. Failing to get meaningful consent is a breach of privacy and a breach of trust. There should be regular audits including user testing to ensure that consent meets the OAIC standards.

Finally, data sharing must ensure that personal information can never be recovered. The Statistical Linkage Key used by various Government departments is relatively simple to crack and accordingly personal information can be discovered with ease. All use of this process must be abandoned and replaced only with effective de-identification.

Recommendations:

1.There should be a review that covers what data is to be shared and including why that data should be shared. This review should be consultative and transparent.

2.The purposes for sharing information need to be underpinned by a commitment to privacy.

3.The Data Commissioner needs to have robust enforcement powers which it is willing to use.

4.Any data sharing requires disclosure. There needs to be a statement that is designed in an accessible plain language format which sets out what is being shared, why it is being shared and how it is shared. This disclosure statement must be mandatory.

5.Any data sharing that involves personal information must only be shared with meaningful consent. That consent must not be bundled, must be in plain language and be prominent. Consent should be audited and user tested.

6.The Statistical Linkage Key does not represent any type of effective de-identification. It can easily be reverse engineered and needs to be abandoned and replaced with effective de-identification

Scope

3. Should the scope be broader or narrower?

The Foundation endorses coverage of the Commonwealth public sector -

- Commonwealth entities and companies as per the *Public Governance, Performance & Accountability Act 2013* (Cth)
- all data collected by those bodies
- all data generated by those bodies.

That endorsement is subject to privacy protection as noted above and to reasonable exceptions regarding national security, law enforcement and contractual obligations.

The breadth of coverage is principles-based: the default position is that data held by the Commonwealth can be released, subject to systematic minimisation of risks and respect for individuals who have not had a choice to provide that data.

With respect to access to justice through data sharing it is desirable that the Commonwealth provide funding for the national not-for-profit austLII information service. If the intention of the proposed legislation is to facilitate government accountability and other social goods that funding will directly complement the DS&R statute.

The Foundation notes concerns that some agencies may seek to erode openness by relying on contractual restrictions when buying in data. This should be addressed through the Commonwealth procurement framework and oversight by the Data Commissioner discussed elsewhere in this submission.

4. Are there entities that should be included or excluded from scope? How would this be justified?

There should be no blanket restriction on types of entities. Such a restriction is not necessary, given scope on the basis of national security or other substantive grounds that should be directly evaluated by the Data Commissioner (and appropriately considered by the Advisory Council), for exclusion of particular data sets. Sectoral exclusion reduces the accountability that is a key rationale for the data sharing regime.

5. Should any specific categories of data be specifically out of scope? How would this be justified?

From the privacy perspective the salient issues are –

- the nature of the data and its consequences, including the likely incidence and severity of harms
- the transparency and thus accountability of data sharing activity

rather than the particular entity as custodian, repository or end-user.

The Foundation considers that the legislation and its implementation should permit the sharing of data about individuals to the extent that there is a compelling public good in that sharing within government. Public good is not the same as bureaucratic convenience.

Sharing within government must accordingly be embedded within a forward-looking and robust legal and administrative framework. That framework requires greater resourcing of privacy functions within agencies and the OAIC (along with a cultural change) if the national Privacy Commissioner is to operate effectively in partnership with the Data Commissioner. It requires restrictions on the release by officials or ministers of personal information regarding people who have complained about the performance of government, a release that is abhorrent and that is contrary to government accountability but has been disquietingly endorsed by the OAIC.

There is **no** rationale for unilateral disclosure to the private sector of data that is personally identifiable or that might be readily re-identified. Any data about individuals must only be released on a robustly and effectively de-identified basis or with the express consent of the individual to who that data relates.

The Foundation reiterates concerns that public and private sector entities holding personal data, including leading government bodies in Australia and overseas that claim to embody best practice, have historically misunderstood risk and failed to anticipate/mitigate serious harms. Assertions that re-identification will not take place or will not be serious are, with respect, either naive or disingenuous and those contrary to the Issue Paper's emphasis on trust. The current controversy regarding implementation of MyHR demonstrates both that there is value for officials in taking on board advice from civil society bodies as centres of expertise and that failure to actively anticipates problems increases administrative costs by eroding trust.

The default position for sharing, other than in closely defined exceptional circumstances, should be disclosure of the sharing activity.

6. Should exemptions, for example for national security and law enforcement, occur at the organisational level or for specific data categories?

Exclusions should be for data categories rather than on an agency by agency (national security/law enforcement entity) basis.

7. Are there instances where existing secrecy provisions should prevail?

Existing provisions under the FOI and other legislation should be reviewed but prima facie might be retained.

The purpose test

8. Do you agree with the stated purposes for sharing data?

The Foundation considers that the stated purposes **must** be contextualised in the legislation through an express reference to respect for privacy.

In essence, the purposes are high level statements. They are so broad as to justify activity that is inappropriate because for example it disregards the recognition, in a range of existing statutes and in common law, of privacy as a core value of the liberal democratic state and of public administration.

It is fundamentally important that any erosion of the private sphere must be clearly proportionate rather than a matter of administrative convenience or institutional advantage. The Foundation acknowledges insights offered in the Productivity Commission's report and in statements by, for example, the Digital Transformation Agency. However, those insights embody a particular ideology about economic values as the determinant of political legitimacy and test of public policy. That ideology is potentially at odds with Australian values regarding non-interference in the private sphere and government as a servant rather than master.

In isolation the purpose test is regrettably inadequate. It is contrary to the social licence that underpins the mandatory collection of data from/about all Australian residents and organisations, and the funding by those entities of government that enables agencies to purchase data. It is not justified through reference to the same model in NSW and Victoria.

The test must be clearly linked to respect for privacy in the legislation and in practice. The latter is important given the history of Ministers and senior executives reading legislation selectively and uncertainty about whether the Data Commissioner will have effective oversight of data sharing activity.

As stated above, the Foundation sees benefit in data sharing that respects privacy through for example rigorous and effective de-identification and that is embedded within an effective transparency framework. Legitimate public data sharing is as much a matter of *how* sharing is affected rather than merely the projected benefits of sharing or the authority of the entity seeking the data.

9. Are there any gaps in the purpose test that would limit the benefits of public sector data use and reuse?

See immediately above

10. What further detail could be included in the purpose test?

The Foundation looks forward to sighting the Exposure Bill and would welcome direct discussion with the Department regarding this question.

One basis for concern has been the interpretation by the Office of the Australian Information Commission – through summary responses to complaints and through interpretive guidelines – regarding the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth). The APPs have been read down with 'reasonable practice' being construed on a lowest common denominator basis. FOI

access to internal Privacy Commissioner documentation has also demonstrated the Commissioner's office has a tendency to regulatory capture by for example particular research interests.

Recommendations:

1.Each element of the purpose test will need to be glossed in readily accessible guidance by the Commissioner and

2.The legislation must provide for timely readily accessible disclosure of what data is being shared, why it is being shared, how it is being shared, and who is sharing.

11. Should data be shared for other purposes? If so, what are those purposes?

The proposed purposes are sufficiently broad, depending on the interpretation discussed in relation to **Q 11** above.

12. Should there be scope to share data for broader, system-wide purposes?

No. A rationale has not been made for an even broader sharing regime.

13. Should the purpose test allow the sharing of data to administer or enforce compliance requirements?

This appears to be covered under Purpose 2.

The Foundation notes that existing legislation often specifically allows for sharing across government entities of personal data for a wide range of law enforcement and other purposes. That sharing is not transparent but is potentially disproportionate. The Foundation would accordingly welcome a transparency requirement under the proposed legislation that would address civil society concerns regarding the government's own practices, consistent with social licence comments made above and with criticisms by the Ombudsman, the Australian National Audit Office and parliamentary committees regarding bureaucratic opacity as an impediment to accountability and thence process improvement.

Data safeguards

14. Is the Five-Safes framework the appropriate mechanism to ensure data is safeguarded?

The Foundation welcomes the recognition in the proposed Five-Safes framework of the significance of privacy at an abstract level and the realities of data sharing practice, for example the prevalence of data breaches in the public/private sectors and the under-estimation of the ease with which sensitive personal data might be re-identified.

It is imperative that the proposed legislation enshrine the Five-Safes in direct relation to the Purpose Test and to compliance with the legislation. In particular, the Data Commissioner must have the expertise and formal authority to critically evaluate data sharing activity and to intervene on a timely basis where an entity has disregarded or misunderstood the Five-Safes. It is also imperative that any data custodian is adequately educated on a range of issues including, the manner in which trust is assessed and quantified, the access environment is safe and understood, and to ensure that data cannot be re-identified.

15. Are there any additional safeguards that should be applied?

See comments re **Q. 19** below.

16. Are there any instances when the Five-Safes could not be applied?

No. The Five-Safes must be enshrined as integral to the legislation and given effect through practice at the agency, Commissioner and external end-user levels.

Recommendation:

The Five Safes must be enshrined in legislation

17. Is the Five-Safes appropriate when data is shared and used for the specific purposes in the purpose test above?

Subject to the Foundation's above comments, Yes.

18 How should the responsibility for managing risks be shared in the framework?

The Foundation considers that responsibility is of critical importance. Effective risk identification, anticipation and response involves responsibility on the part of Commonwealth entities or their proxies that collect data, that process data, that store data, that distribute data and that use data. It also requires responsibility on the part of the Commissioner and the OAIC, along with advice from entities such as the National Health & Medical Research Council and the Australian Signals Directorate. Risk management and thence the legislation will be ineffective if responsibility rests with the Commissioner; the legislation must ensure 'buy in' on the part of agencies and compliance by external users of data (irrespective of mechanisms such as strong de-identification).

The Foundation notes wide-spread concerns regarding the effectiveness of the OAIC, which has misread the responsive regulation discussed at the July 2018 consultation in Canberra and has therefore unduly weight its response to risk by emphasising conciliation rather than more persuasive parts of the enforcement pyramid. In building a data sharing regime that is positive and forward looking the Commissioner must

- be empowered to push data sharers towards best practice, something that is different from the 'reasonable practice = lowest common denominator' model used by the OAIC
- have the culture and technical resources for meaningful supervision and, where necessary, intervention

Responsibility will be substantively enhanced through the transparency requirement identified throughout this submission.

A key concern regarding responsibility is the uncertain relationship between the Privacy Commissioner (OAIC) and the Data Commissioner. The Foundation expects that this will be clarified in the Exposure Draft and that the architecture for data sharing will minimise confusion and scope for regulatory arbitrage.

19. How would you envisage Five-Safes principles be applied over the life-cycle of data to ensure data safeguards are continually met?

It is axiomatic that the Commissioner should be able to seek independent reviews of agency practice once data sharing has occurred. Contractual or other licencing agreements must expressly provide for such reviews.

This submission has emphasised timely and readily accessible disclosure regarding data sharing (e.g. what was shared, to whom, and why). That disclosure enables public identification and evaluation of the extent to which data safeguards have been implemented and evaluation of their effectiveness.

The submission has also indicated the value of truly inclusive and informed Advisory Council that does not embody regulatory capture by data users and is able to foster a regime in which data safeguards are continually met. The Foundation notes that the problems evident with the My Health Record regime were readily identifiable prior to July 2018 and indeed had been recurrently highlighted by both civil society organisations and by legal academics, information technology specialists and others.

Given that a rationale for data sharing is enhanced public administration the performance of government and its proxies/partners can be significantly improved through transparency regarding data sharing activity and by taking on board advice from outside government about the framework for that activity.

Open Government involves Ministers, the Parliament and the bureaucracy listening to and acting on advice 'from the bottom' rather than merely distributing data from the top.

20. Under what circumstances should trusted users be able to access sensitive data?

In circumstances where they have made an enforceable commitment to comply with the Five-Safes and more broadly have demonstrated that they have the necessary human/technical resources and culture.

Public sector data sharing arrangements

21. Would this arrangement overcome existing barriers to data sharing and release?

The Foundation has two responses to this question.

The first is that a properly articulated and implemented framework will address perceived barriers. The Foundation accordingly looks forward to sighting the Exposure Bill and would be happy to meet with the Department regarding issues highlighted in this submission.

The second response is that some barriers to data sharing (which the Foundation construes as including release) are indeed appropriate. That appropriateness is evident in both statute law and in case law. The proposed data sharing regime should not assume that the removal of barriers – through for example an omnibus amendment of a wide range of Commonwealth statutes – is a legitimate and politically acceptable end in itself.

The Foundation thus commends the Department's exploration of a multi-factor Purpose Test that embraces privacy protection. The Department should critically review claims by agencies or non-Commonwealth entities that are based on bureaucratic convenience rather than substantive public good or that are founded on institutional advantage.

22. Would streamlined and template agreements improve the process?

The Foundation believes that it is feasible to develop a suite of agreements that covers different types of data (not all of which will relate to individuals), different types of uses and different capacity on the part of different actors. The Foundation has emphasised ongoing community consultation and transparency regarding data sharing activity in the expectation that this will foster ongoing review and process improvement. Experience over the past two decades demonstrates that organisation should both look ahead and look back, learning from experience rather than assuming that best practice in data management is a matter of 'set and leave'.

23. Do you agree that data sharing agreements should be made public by default?

Disclosure is a key accountability mechanism and one that will foster trust in the overall regime. It should be specifically mandated, with a requirement that information about data sharing activity be provided on a timely, sufficiently detailed and accessible basis.

That provision is a corollary of the social licence for the sharing of data that is mandatorily acquired or acquired using public funds. There is no principled basis to exempt agencies or partners from disclosure. The procurement framework should specify that agencies cannot opt out of disclosure through contract or a deed.

Recommendation:

It should be mandatory for data sharing agreements to be made public.

24. What level of detail should be published?

As indicated above, disclosure should be specific and for example include –

- identification of the data set, such as how it was created and what it covers
- whether the data was collected on a mandatory basis (inc identification of the statute)
- which entity has access to the data set
- how the data set will be used
- what is the rationale for that use
- whether data was licenced by simple contract or deed
- pricing
- any restrictions on re-use/re-sharing
- whether sharing was on a one-off or ongoing basis
- whether personal data was de-identified and the extent to which de-identification was undertaken
- whether the recipient of the data has accreditation.

In essence, disclosure should on a timeliness and specificity sufficient to enable effective oversight by the Commissioner, ANAO and Parliamentary committees as well as independent scrutiny by for example scholars of public administration and civil society organisations such as the Australian Privacy Foundation. That disclosure is an acceptable cost of government and not one to be evaded on the basis of budget stringencies.

In disclosing sharing of data sets regarding individuals it will be necessary to identify the characteristics of the data, e.g. name, age, location, TFN and other attributes rather than for example 'client data' or 'demographic data set 2015-2018'.

25. What else should a data sharing agreement contain?

Evaluation will be assisted through inclusion of information in the agreement – and disclosure of that agreement – of information that is sufficient to provide the basis for assessment by the Commissioner and other stakeholders of the performance of the entities engaged in data sharing and, by extension, of the effectiveness of the overall data sharing regime. That information can be used prospectively and retrospectively

26. What other transparency mechanisms could be mandated?

See above.

Accreditation

27. How long should accreditation as an ADA or Trusted user last?

Accreditation should be for a three-year period

28. What could the criteria for accreditation be?

Accreditation should reflect the attributes noted below and those in the Commonwealth procurement framework regarding information services, which is informed for example by advice from the Australian Signals Directorate.

It should also reflect the type of data (construed in terms of potential harm and respect for individuals).

The Foundation notes suggestions that a stringent regime will either inhibit public administration (in particular law enforcement) or disadvantage small research institutions. It considers that a persuasive case has not been made to support claims that administration will be substantively inhibited. Small research institutions consistent with emerging national policy regarding the tertiary sector may offset weaknesses by participating in consortia. Commercial entities wanting access to data that has been collected by the Commonwealth on a mandatory basis should be expected to meet particular standards and not for example assume a broad claim of potential innovation is sufficient from dispensation regarding obligations to protect sensitive data.

29. Should there be review rights for accreditation?

Yes, consistent with notions of natural justice.

Review activity should be identified in the Commissioner's Annual Report at a level beyond a statement that x review was undertaken at y time of entity z.

30. Should fees be payable to become accredited?

Yes, accreditation costs should be recovered.

31. Is the Australian Government Charging Framework fit for purpose in this context?

The framework should be reviewed as part of the establishment of the Commission, noting overseas experience regarding difficulty in appropriate pricing of life sciences and other data.

The Commissioner

32. Are these the right functions for the National Data Commissioner?

See above.

Clarification of the relationship between the Data Commissioner and other entities such as the national Privacy Commissioner and FOI Commissioner is necessary.

33. What review powers should the National Data Commissioner have?

The Foundation considers the Commissioner should have and be prepared to use powers to require data sharers to disclose data sharing activity, to commission independent investigation on its behalf regarding that activity, to refuse authorisation of data sharing activity on the basis that it is contrary to the legislation and to suspend activity that it reasonably believes is contrary to the legislation.

Recommendation:

The National Data Commissioner should have wide powers including powers to require details of data sharing, to commission independent investigation, refuse authorisation, and suspension powers that are effective immediately.

34. Should the NDC have the power to conduct an investigation into system-wide issues?

Yes, this power is essential. The Commissioner must have the resources necessary for investigation on an own-motion basis on a data set or system-wide basis rather than merely in response to complaints.

The Commissioner should be required to publicly report on investigations, though Parliament, within six months. (That report might be provided on an interim basis.) The report should be sufficiently detailed for external assessment, thus for example moving beyond OAIC practice that on occasion has comprised a simple statement that an investigation was undertaken.

The Commissioner's annual report should tabulate investigatory activity and specifically identify agencies/other parties. That reporting provides a practical mechanism for ministerial and official accountability.

Recommendation:

The National Data Commissioner must have the power to investigate and report on systemic issues. This needs to include referral powers for remedy and enforcement.

35. What other actions could the NDC be able to take?

See above.

36. Are there other ways community values and expectations can be captured and addressed?

A salient way is an inclusive Advisory Council in which there are sufficient civil society representatives to articulate community values and expectations. Indications that civil society will have only two representatives on a ten-member Council are disquieting.

Recommendation:
Any advisory council must include 5 civil society representatives to ensure there is adequate representation of the Australian people.

37. What aspects should be taken into consideration when considering consequences for non-compliance with the DS&R Bill?

There needs to be real and serious consequences for non-compliance with the DS & R Bill. The current proposal is to give immunity against criminal liability for any data custodians acting "in good faith with a genuine belief that disclosure is required or permitted under the DS & R Bill." This must not extend to civil liability.

There must be legal liability for releases of data that harm individuals. This is required to ensure there is trust in the system. Liability must flow from harm. If it is not set up in this way then there is insufficient incentive to ensure compliance. At a minimum there must be liability for negligence although the Foundation argues that this would be a much lesser standard.

We also refer to the Australian Law Reform Commission Report[1] which recommended enacting legislation to deal with serious invasions of privacy. Those recommendations have not been actioned. However, now that there is a proposal for data sharing it is now essential that those recommendations are enacted to provide a clear remedy for individuals affected by serious invasions of privacy.

Recommendations:

1. There must be legal liability for breaches of the DS & R Bill. Individuals should be able to seek compensation for harm

2. The ALRC Report recommendations in relation to serious invasions of privacy should be enacted urgently to give individuals access to justice in the event of harm from data releases

38. Should the consequences differ depending on the type of data involved or the type of misuse, e.g. harsher penalties for intentional misuse?

Yes. See below, where the Foundation suggests that the type of data, the significance of misuse and intention should be taken into account.

The legislation should drive best practice in data sharing by providing for public condemnation regarding negligence.

39. Should penalties be strict liabilities?

Yes.

[1] https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf

40. What would be an appropriate penalty for intentional misuse of data?

The Foundation notes recent comments by representatives of the Australian Competition & Consumer Commission (ACCC) about the operation of the responsive regulation regime under the *Competition & Consumer Act 2010* (Cth) and the importance of increasing penalties against corporations and executives to deter misbehaviour and signal social disapproval. The penalties for intentional misuse of data by entities outside the Commonwealth government should include fines and extend to criminal sanctions against key decisionmakers. Those penalties should reflect the nature of data, with for example deliberate misuse of sensitive personal data by an Australian or overseas-based entity necessarily being addressed more severely than a geospatial data set that is of transient value.

The legislation must impose significant penalties for negligence in data sharing rather than merely intentional misuse.

It should recognise that not all data sharers have the same capability, e.g. some have the infrastructure and human resources to actively identify and address risk through use of strong encryption, staff vetting, secure premises and so forth whereas others do not. Commonwealth guidelines implementing the legislation should however address that differentiation by managing risk through restrictions on provision of sensitive/high value data to entities that of an unknown/uncertain capability or that are reasonably deemed not to have that capability.

Recommendations:

There must be penalties for both intentional misuse and negligence. The penalties for intentional misuse of shared data need to be significant to act as an incentive to ensure data is only shared in accordance with the law. There should also be penalties for negligence.

41. How would responsibility for misuse of data be shared across the data system?

See above regarding **Q 18**. The Foundation notes concerns regarding both regulatory incapacity on the part of the OAIC (benchmarked against for example the ACCC and ACMA) and the potential for confusion or evasion on the part of stakeholders.

42. To what extent should there be a complaints mechanism and how should it work?

The Foundation considers that non-substantive complaints and queries will be minimised through the disclosure regime discussed on preceding pages of this submission.

The legislation should allow for complaints by the general public – in the first instance to the specific data sharer/s and then to the Commissioner – that sharing has taken place outside a formal agreement or that sharing is contrary to the Purpose Test and Five-Safes. The legislation should provide for the Commissioner to investigation in response to a complaint and more broadly to initiate own motion investigations on a timely basis, with a report on that investigation being published on a timely basis. (A benchmark in that respect is the slow response, often triggered by media coverage, on the part of the OAIC over several years and attributed to both that agency's resourcing and culture.)

The Commissioner should have both the authority and willingness to suspend specific data sharing activity in instances where there is a reasonable belief that the activity is contrary to the data sharing legislation.

Recommendations:

1. There must be a complaints mechanism for people to complain about misuse of data.

2. The complaints mechanism should be to make a complaint to the data sharer then if the complaint is not resolved to the National Data Commissioner

3. The National Data Commissioner must investigate the complaint

4. The National Data Commissioner must have the power to award compensation for breaches and harm caused

43. Should a complaints mechanism provide for complaints by the public?

Yes, this is essential and is consistent with civil society expectations about responsible government.

If you have any questions please do not hesitate to contact Bruce Arnold or Kat Lane.

Yours sincerely

Bruce Arnold
Vice-Chair
Australian Privacy Foundation
P: 02 62012710
E: vicechair1@privacy.org.au

Kat Lane
Vice-Chair
Australian Privacy Foundation
P: 0447620694
E: vicechair2@privacy.org.au