Submission No 2

INQUIRY INTO DIGITAL RESTART FUND BILL 2019

Organisation: Information and Privacy Commision NSW

Date Received: 13 December 2019

information and privacy commission
new south wales

Enquiries: Philip Tran

Our reference: IPC19/A000434

The Director,
Portfolio Committee No. 6
Parliament House
Macquarie Street, Sydney NSW 2000

Attention: The Director, Portfolio Committee No. 6
By email: portfoliocommittee6@parliament.nsw.gov.au

Dear Director,

Inquiry into the provisions of the Digital Restart Fund Bill 2019

The purpose of this submission is to provide comments to the Inquiry into the provisions of the Digital Restart Fund Bill 2019.

Introduction

Digital Restart Fund Bill 2019

The Bill establishes the Digital Restart Fund (the Fund) for the purpose of providing funding for digital and information and communications technology initiatives across the government sector.

The purpose of the Digital Restart Fund, described in clause 6 of the Bill, is:

'...to support digital and information and communications technology initiatives across the government sector, and for that purpose, to fund projects that:

(a) develop and implement digital and information and communications technology products or services that, for the purpose of improving the delivery of services by government agencies and related interactions
    (i) identify the actions required to be taken by an individual (or on the individual's behalf) in respect of significant events during the individual's life, and
    (ii) record related interactions between the individual (or on the individual's behalf) and government agencies or non-government entities or other bodies or persons connected with the delivery of services by a government agency, and
    (iii) identify impediments to the delivery of related services by government agencies and develop and implement solutions to those impediments, or

(b) develop and implement digital and information and communications technology products or services that are capable of being used by multiple government agencies in a cost-effective manner, or

(c) optimise existing technologies, applications, computer systems or processes used by government agencies to improve the functionality and operational life of those technologies, applications, computer systems or processes, or

(d) provide persons employed in or by a government agency with education, training and information relating to digital and information and communications technology.'

Under clause 7 of the Bill, the Minister controls and manages the Fund.

Scope of the Commissioners' submission to the Committee

Information access and privacy issues arise in respect of the initiatives and projects that could be funded by the Fund. The Commissioners address these issues in this submission.

The Commissioners consider that initiatives funded by the Fund should promote and embed information access and privacy considerations into their design. In its current form, the Commissioners are concerned that the Bill establishes the Fund and describes the purpose of the Fund, but does not provide for the criteria in which initiatives are to receive funding. Clause 9 of the Bill says money is payable from the Fund for all or part of the cost of a project that promotes the purpose of the Fund and is approved by the Minister on advice of the Secretary. The Minister may also obtain advice under clause 11 in exercising his functions.

The Commissioners suggest there is scope for the Bill to expressly safeguard information access and privacy rights, whether as a condition of funding or that, for example, the Minister is required to take advice about privacy and information access controls and mechanisms embedded in the proposed project.

Rights oversighted by both the Information and Privacy Commissioners are frequently impacted by new service delivery approaches. Maintaining trust and confidence that rights will be preserved will ensure public acceptance in the utilisation of these new models for service delivery and contribute to informed decision making by government. Under extant legislation enshrining these rights, modifications and exceptions operate, for example, public interest directions and privacy codes of practices under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). These provisions are transparent and accordingly, accountability mechanisms are maintained.

The Commissioners suggest the Bill include a public interest test so that projects are funded where they promote the public good/interest and in a way that preserves existing information access and privacy rights. The *Government Information (Public Access) Act 2009* (NSW) (GIPA Act) enshrines a public interest test and this provides a mechanism with which to balance rights and interests. Privacy and information access rights must be considered in the context of related considerations including cyber security, customer value, ethics and technical operability. Where those fundamental rights are abrogated by a proposed initiative/project, the reasons for the decision to proceed with funding should be transparent and explained by the Minister.

Information Access

Agencies have statutory obligations under the GIPA Act to:

- interpret and apply the Act to further its objects, including to open government information up to the public
- exercise discretion to facilitate and encourage prompt access to government information, at the lowest reasonable cost
- uphold the general principles of open government information.

Object of the GIPA Act

The object of the GIPA Act is to open government information to the public and in doing so maintain and advance a system of responsible and effective representative democratic government that is open, accountable, fair and effective. This object is to be realised by agencies authorising and encouraging proactive public release of government information (section 3(1)(a)); and by giving members of the public an enforceable right to access to government information (section 3(1)(b)).

Subsection (1)(c) under section 3 of the GIPA Act provides that access to government information is restricted only when there is an overriding public interest against disclosure.

It is the intention of Parliament that the GIPA Act be interpreted and applied so as to further its object (section 3(2)(a)); and that the discretions conferred by the GIPA Act be exercised, as far as possible, so as to facilitate and encourage, promptly and at the lowest reasonable cost, access to government information (section 3(2)(b)).

Section 4 of the GIPA Act defines government information as information contained in a record held by an agency. An agency must have an agency information guide which identifies the various kinds of information held by the agency (section 20(1)(d)). The guide must be made publicly available, together with an agency's policy documents (sections 6, 18(a) and 18(c)). What constitutes an agency's policy documents is set out in section 23 of the GIPA Act.

Public Interest Test

Under the GIPA Act there is a general public interest in favour of the disclosure of government information. The GIPA Act provides for a balancing of considerations in favour of and against disclosure, having regard to the public interest. This is known as the 'public interest test'. The test requires consideration of:

1. The presumption in favour of release of government information;
2. Identification of factors in favour of disclosure;
3. Identification of factors against disclosure; and
4. Balancing of factors to determine where the public interest lies.

There is an overriding public interest against disclosure of government information if (and only if) there are public interest considerations against disclosure and, on balance, those considerations outweigh the public interest considerations in favour of disclosure. The balancing of public interest considerations may necessitate consideration of privacy protection principles and the interaction between the GIPA Act and the PPIP Act is well

established within both statutes. The GIPA Act facilitates privacy protection through mechanisms including creation of a new record and redaction of information. Sections 5 and 20(5) of the PPIP Act recognise that the GIPA Act is not limited by the PPIP Act and therefore information may be released under the GIPA Act (either proactively or in response to an application).

The principles set out in section 15 of the GIPA Act guide the application of the public interest test. One principle recognised is that disclosure of information which might cause embarrassment to or loss of confidence in the Government is irrelevant and must not be taken into account.

It is submitted that the public interest test is an enabler in the protection and management of information. Legislation is an important tool for setting out rights and responsibilities. There is scope for a 'public interest test' to be utilised in the regulation of and facilitation (through legislation) of digital government. The definition of 'government information' under section 4 of the GIPA Act extends to all forms of government information held in a record by an agency. This definition has application to information held in digital format.

There will be many interests that need to be balanced in respect of funded digital and information and communications technology initiatives. These interests can include privacy, human rights, security, intellectual property, societal benefits and data monopolies to name a few. It is not clear how these diverse interests would be balanced unless the public interest is clearly defined. As to the Bill, it is therefore suggested that public interest objectives in respect of initiatives to be funded are defined in the legislation.

The Information and Privacy Commission is currently exploring provision of advice to agencies and the Government through development of a public interest framework and a digital audit tool.

Preservation, assurance and assertion of rights in digital government

The application of technology to provide services, including the use of artificial intelligence, is an increasingly prevalent feature of service delivery by government. Direct and facilitative service contracts are characteristic of digital solutions in which a number of entities are involved in the provision of services to the public. There are identified barriers to access to information that derives from automation including restrictive licencing arrangements and explicability of algorithms. In these circumstances the assertion of legal rights can be compromised. One solution to address this challenge is providing access to information. In upholding the right to access information individuals can understand and have confidence in how decisions are made and, importantly, assert their rights in respect of those decisions.

The GIPA Act places an obligation on agencies to ensure that citizens have access to information through mandatory and authorised proactive release of government information, and through informal and formal access application pathways. The Bill could include provisions that ensure that in controlling and managing the Fund, the Minister takes advice about the information governance arrangements in respect of the initiative/ project. In addition, the Bill could include criteria that must be met to the Minister's satisfaction and upon which funding is conditional. The criteria could include evidence of information governance arrangements in respect of the project, such as application of a public interest test, or rights impact assessment or an operational audit to identify risks and rights impacted. In this regard, it is important that agencies factor into their project

planning that information on their proposed projects could be subject to the GIPA Act and agencies should conduct an assessment of the impact of their proposed projects on the right to information as enshrined in the GIPA Act.

Preservation of the principles of open government under significant government partnership and outsourcing arrangements

The Information Commissioner expects agencies to have regard to the application of section 121 of the GIPA Act when entering into contracts with private sector persons to ensure that certain information held by contractors is designated as government information and subject to the GIPA Act.

A reference in the GIPA Act to government information held by an agency is a reference to information contained in a record held by a private sector entity to which the agency has an immediate right of access (clause 12(1)(b) of Schedule 4 to the GIPA Act). Section 121 of the GIPA Act contains mandatory requirements for certain government contracts to provide for immediate rights of access to information held by private sector contractors.

Where such contractual rights exist, an access application under section 9 of the GIPA Act can be made to the agency for that information, and a person has a legally enforceable right to be provided with access to the information in accordance with Part 4 of the GIPA Act unless there is an overriding public interest against disclosure of the information.

Section 121 of the GIPA Act applies in circumstances where an agency enters into a contract with a private sector entity to provide services to the public on behalf of the agency.

Subject to certain exceptions, section 121 requires government agencies to ensure that their contracts provide them with an immediate right of access to information:

- relating directly to the performance of services by the contractor
- that is collected by the contractor from members of the public to whom it provides, or offers to provide, the services, and
- that is received by the contractor from the agency to enable the contractor to provide the services.

Section 121 mandates the inclusion of a clause to permit access to information held by the contractor. Despite the mandatory requirements of section 121, where there are no contractual arrangements in place and no immediate right of access to information, information in the possession of a contractor may not be government information held by an agency for the purposes of the GIPA Act.

Agencies should consider how information associated with government contracts is transparently accessible, whether the contractor is providing a service to the public or undertaking an activity that assists the agency to provide a service to the public. The Information and Privacy Commission has published the following guidance to promote awareness and understanding of agency obligations under section 121 of the GIPA Act:

- Contractor's guide to section 121 of the GIPA Act
- Agency's guide to section 121 of the GIPA Act

Division 5 of Part 3 of the GIPA provides for open access requirements in respect of government contracts with the private sector. Under section 27, an agency is to keep a register of government contracts that records information about each government contract to which the agency is a party that has (or is likely to have) a value of $150,000

(including GST) or more. It is feasible that significant new initiatives that may be funded by the Fund cost less that the $150,000 threshold and therefore a lack of transparency and accessibility in respect of those contracts arises. For example, the Information Commissioner is aware of a matter in the NSW Civil and Administrative Tribunal involving the calculation of a rental subsidy using an algorithm that is inaccessible to government or citizens through a contract that is not required to be disclosed under the GIPA Act because it does not meet the monetary threshold for disclosure.

Privacy

NSW public sector agencies have legal obligations under the *Privacy and Personal Information Protection Act (1998)* (NSW) (PPIP Act) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act) which they must abide by when they collect, store, use or disclose personal or health information.

With reference to clause 6 of the Bill, the Fund's purpose is directed to developing and implementing digital and information and communications technology products or services for individuals. Therefore, there is potential for Digital Restart projects to collect significant amounts of personal and health information.

Further, the focus on improving service delivery between government agencies and individuals potentially leads to the sharing of personal or health data among NSW agencies. Under the PPIP Act, personal information may only be used or shared for the purpose for which it was collected, or for a secondary purpose if an exception applies.

Agencies must determine whether the sharing of personal information with a third party is compatible with the original purpose for which it was collected and the privacy policy and/or notice given to the individual. If it is not compatible, the data that contains personal information must be de-identified. If the data is reasonably de-identified, the modified data may no longer trigger privacy legislation. That said, risk of re-identification is also recognised, see for instance: Office of the Victorian Information Commissioner's report on disclosure of myki travel information.

The Privacy Commissioner expects that before agencies are granted funding for their Digital Restart projects, they explain how they will comply with the PPIP Act and HRIP Act (if applicable). This can be done by way of a privacy impact assessment (PIA) which identifies privacy risks of a program and how those risks can be mitigated. Privacy compliance should be incorporated into the design of the project for which funding is sought from the Fund. These concepts are explained further below.

Privacy by Design

Privacy by Design (PbD) is a specific approach to privacy, developed by Dr Ann Cavoukian, the former Privacy and Information Commissioner of Ontario, Canada, in the 1990s.

The PbD framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010. The U.S. Federal Trade Commission recognised PbD in 2012 as one of its three recommended practices for protecting online privacy in its report entitled, *Protecting Consumer Privacy in an Era of Rapid Change*. More recently, PbD has been incorporated into article 25 of the European Union General Data Protection Regulation.

Privacy by Design is a methodology that enables privacy to be built into the design and structure of information systems, business processes and networked infrastructure. PbD

aims to ensure that privacy is considered at all stages of the project life cycle from conception through to development and implementation of initiatives that involve the collection and handling of personal information. It positions privacy as an essential design feature of public sector practices and shifts the privacy focus to prevention rather than compliance.

The PbD methodology is built around seven foundational principles:

- **Proactive not reactive, preventative not remedial:** The PbD framework is characterised by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur.
- **Privacy as a default setting:** PbD seeks to deliver the maximum degree of privacy by ensuring that personal information is automatically protected in any given IT system or business practice, as the default.
- **Privacy embedded into design:** Privacy measures are embedded into the design and architecture of IT systems and business practices. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system, without diminishing functionality.

- **Full functionality: positive –sum not zero-sum:** PbD seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum (either/or) approach, where unnecessary trade-offs are made. PbD avoids false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both.
- **End-to-end security – full lifecycle protection:** PbD extends securely throughout the entire lifecycle of the information involved. This ensures that all information is securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion.
- **Visibility and transparency – keep it open:** PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is operating according to the stated promises and objectives, subject to independent verification. The individual is made fully aware of the personal information being collected, and for what purposes. All the component parts and operations remain visible and transparent, to users and providers alike.
- **Respect for user privacy – keep it user centric:** PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

The requirements of the Australian Privacy Principles under the *Privacy Act 1988*, particularly the requirement for open and transparent management of personal information under APP 1 reflect the Privacy by Design Framework. Privacy by Design has also been adopted as a policy by the Office of the Victorian Information Commissioner.

The application of the Privacy by Design framework is not a requirement under the PPIP Act. The IPC recommends that agencies apply the principles of PbD to their projects as a condition for funding.

A PIA can often identify and mitigate the challenges that are encountered in implementing PbD to their project.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) allows an agency to identify and address privacy risks associated with their project before it is too late. A PIA is more than achieving regulatory compliance - it enhances the quality of information before decision makers and demonstrates that a project has been designed with privacy in mind.

The timing of a PIA is crucial. A PIA should be conducted early enough so that it can genuinely affect project design, yet not too early as to prevent you from obtaining the necessary information about the project to adequately assess any privacy risks.

There are seven key elements to achieve an effective PIA. A PIA should be:

- **Integral to an organisation's governance:** the PIA should be integrated into an organisation's governance structure and have clear guidance on who has responsibility over the PIA;
- **Fit for purpose:** the PIA should be commensurate with the potential privacy risks associated with the project;
- **Comprehensive:** the PIA should cover all privacy issues, not just information privacy. A PIA should also consider whether change is required in supporting documentation such as Privacy Management Plans, human resource policies or training material to accompany project implementation;
- **Available:** the PIA report should be publicly accessible as this demonstrates accountability. Where this is not possible, consider releasing a PIA summary report to notify and seek feedback on privacy issues;
- **Enables compliance:** the PIA must address all legal obligations, including under privacy legislation, namely, the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) where relevant;
- **Ongoing:** the PIA should contain an ongoing review mechanism to assess privacy issues throughout the life cycle of the project; and
- **Constructive:** the PIA should support your organisation's privacy culture and reference your organisation's risk management process.

Preservation of accountability and digital governance

In respect of digital and information and communications technology initiatives it is important that following issues are understood:

- How is government data managed, who uses it, and for what purposes?
- Does the initiative involve technological, algorithmic and artificial intelligence systems that impact citizens lives?
- How does the initiative ensure the ability to question and change unfair, biased or discriminatory systems?
- How will access to digital services on equal terms be ensured?
- What is the impact on managing digital infrastructures and data as a common good?
- How does the proposal promote public interest objectives?

- How are digital service standards ensured and utilised?
- What skills/capability might be required of the public sector and citizens?

Understanding the above issues will ensure that privacy and information access rights are safeguarded, and initiatives are developed in the public interest.

Conclusion

The Information Commissioner and the Privacy Commissioner recognise that the development and implementation of new technologies and modes of service delivery have the capacity to enhance the citizen experience of government. At the same time, these developments introduce potential new risks of harm. Maintaining the trust and confidence of citizens that their rights will be protected as these projects develop will contribute to the success of the projects.

The Commissioners recommend that the Bill include express safeguards for information access and privacy rights. These safeguards could be in the form of express legislative considerations as a condition for funding, or a requirement for the Minister to take advice on information access and privacy controls and mechanisms for each project.

The Commissioners recommend that the Bill include a public interest test so that projects are funded where they promote the public good/interest and in a way that preserves existing information access and privacy rights. A 'public interest test' may be seen as an enabler in the protection and management of information. The Bill should include defined public interest objectives in respect of initiatives to be funded under the Fund.

Transparency in decision making, including clear legislative considerations in the decision-making process contributes to open democratic government. Clear provisions requiring the consideration of safeguarding information access and privacy rights as part of the project design, and as a condition for funding contributes to such transparency.

As an independent regulator with expertise in information access and management, data governance and privacy, the Information and Privacy Commission welcomes the opportunity to make a submission to the Committee.

If you have any questions please contact Philip Tran, A/g Senior Project Officer

Yours sincerely

Elizabeth Tydd
Information Commissioner

Samantha Gavel
Privacy Commissioner

12 December 2019