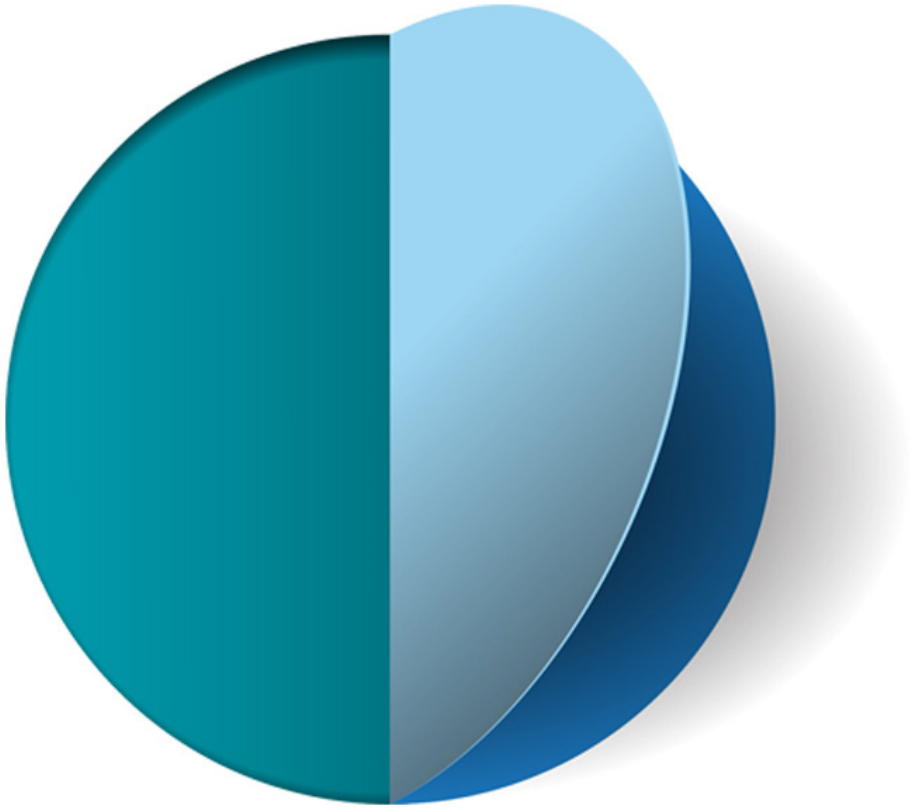
Deloitte.



Open by default

Revisiting open data in government

Introduction

'What Got You Here Won't Get You There' is the title of a popular self-help leadership book first published a decade ago. It could also be the catch cry for open data in government.

Open data in government started about a decade ago, but, with its focus just on making data more open and easily accessible to the public, the results have been underwhelming. Globally, the reality is that very few government organisations have experienced any of the returns that open data was originally expected to provide.

With a risk-averse culture, many government organisations have been captive to the sum of their fears, focusing on the downside risks and not the citizen and societal benefits from open data.

A binary approach when deciding whether to release data – release publicly or not release – has missed an opportunity to see a range of non-mutually exclusive choices which can be applied to each data set.

But it's time for this narrative to change.

This will require a change in culture in the public service 'to achieve a paradigm shift from 'need to know' to 'responsibility to share'.[1]

It's time for governments' open data strategies to pivot from the practices of the last decade, and adapt to those needed to support the emergence of the open data economy in Australia.

1. Australian Government, Discussion paper, September 2019, page 13

Where it all began

Data is the new capital of the global economy. Open data is one of two major developments, along with big data, that are reshaping relationships between customers, citizens, businesses, governments and society, and their relationship with information.

What is Open Data

Open Data has traditionally referred to data release at no charge. But this restricted definition has passed its use-by data. The introduction of the Consumer Data Right has expanded the use of the term 'Open'. Open banking will commence in February 2020. Open energy and open telecommunications will follow. Open super and open insurance are already being talked about. So the old meaning of the term 'open data' is no longer valid.

Open data is not a binary choice between closed and open data. The degree of data openness is a continuum. We use the term Open Data in government (perhaps even Open Government?) to refer to both data sharing and data release whether this be to the public, to individual citizens, accredited third parties and other government organisations.

Data sharing refers to providing controlled access to data to the right people for the right reasons with safeguards in place.[2]

Data release refers to making information available to the public, the world at large.

Open data is not just about data. Open data impacts the way business and government ecosystems work, tackling the efficiency of markets, competition and supporting government policy.

Open data in government has been around for over a decade in some form both globally and in Australia. In Australia it has historically been driven by separate state government legislation and policies that promote the sharing or release of public data. The proliferation of strategies for leveraging data in government is driven in large part by a desire to enhance efficiency, build civic trust, and create social and economic value.[3]

A decade ago, governments focused on how to make data more open and easily accessible to the public.[4] But while there have been some successes, the outcomes so far, both in Australia and globally, have largely been underwhelming.

Classic principal-agent issues have meant that those incurring the costs of open data, creators and custodians of data, are often different from those who reap the benefits, other government departments, researchers and the public.

Principal or Agent?

The decision on whether and how to standardize or publish a government data set has all the ingredients of a standard principal-agent problem in economics.

Principals (the public, legislators, and, to some extent, executive branch leaders) generally want data to be open because they stand to reap the societal and/or reputational benefits that come from releasing it. However, the decision of whether to standardise or release data is made by an agent

Agents (usually some combination of program managers, information technology professionals, and lawyers) tend to gain little direct benefit from releasing the data – but they could face substantial costs in doing so. Not only would they need to do the hard work of standardisation, but they would incur the risk of reputational damage, stress, or termination if the data they release turns out to be inaccurate, creates embarrassment for the program, or compromises privacy, national security, or business interests.

As a result, even if a political leader wants to share data, there may still be obstacles to doing so.

Source: Deloitte, How CDOs can overcome obstacles to open data-sharing, 2019

Too few valuable data sets have been released. Moreover, simply publishing a data set on an open data portal or website is not enough.[5] Tracking simplistic metrics such as the number of data sets published does not focus on the value that sharing data creates, and can often lead to dysfunctional behaviours, such as disaggregating data sets to hit an arbitrary target of the number of data sets published!

A culture of maintaining confidentiality of data and allowing access to data on a 'need to know' basis has been hard to shift. Today, while there is still much to be done to move to a culture based on 'responsibility to share' and make government data more open, governments are also considering their role in overseeing the types and validity of the data they make available, seeking ways to create greater public value from data, and debating how best to protect privacy and govern data use.[6]

Following a number of reviews, and the 2015 Prime Minister's Public Data Policy Statement, the Productivity Commission was asked to investigate the options for improving the availability and use of data in the Australian economy.

2. Australian Government, Department of the Prime Minster and Cabinet, Data Sharing and Release: Legislative Reform, Discussion paper, September 2019, page 3. Refer https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms
3. Deloitte Center for Government Insights, Managing data ethics: a process-based approach for CDOs, in The Chief Data Officer in Government: A CDO Playbook, 2019. Refer https://www2.deloitte.com/insights/us/en/industry/public-sector/chief-data-officer-government-playbook.html
4. Deloitte Center for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019
5. Deloitte Center for Government Insights, Connecting data to residents through data storytelling, 2019
6. Deloitte Center for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019. Refer https://www2.deloitte.com/insights/us/en/industry/public-sector/chief-data-officer-government-playbook.html

The Productivity Commission noted that the growth in both data generation and usability has the potential to transform the Australian economy – for both the public and the private sectors.

On 1 May 2018, the Australian Government released its final response to the Productivity Commission's Inquiry into Data Availability and Use. The Government committed to reforming data governance to better realise the economic and social benefits of increased data use while maintaining public trust and confidence in the system.[7]

This has resulted in the Consumer Data Right (CDR) legislation in the private sector which was passed in August 2019, and the release in September 2019 of the Commonwealth Government's discussion paper on the Data Sharing & Release legislative reforms as part of the federal government's consultation process leading up to the introduction of the Data Availability and Transparency Act (DATA) in the federal parliament in mid 2020.[8]

Although the ***generation*** of data is an enabler, and the ***sharing and release*** of data are catalysts, it is the ***use*** of data that drives social and economic value, builds trust and enhances efficiency.[9]

Much of the data collected and stored by public sector agencies is only used by the agency that collects it and remains inaccessible to the public.[10, 11] Where it has been shared, this is sometimes done in spreadsheets or in other formats that limit its usefulness.[12] Benefits have been difficult to quantify and sometimes to even identify, whereas the costs are clear.

Government organisations – federal, state, territory and local – have an active role to play in the journey to an open data economy.

In addition to federal open data initiatives, state governments have either or both implemented legislation and developed policies to reform data use, access and sharing processes.

State/Territory	Data Sharing Legislation
NSW DATA NSW PROVIDING ACCESS TO NSW GOVERNMENT DATA	**New South Wales** – The NSW Government Information (Public Access) Act 2009 facilitates public access to NSW Government information. The Data Sharing (Government Sector) Act 2015 (NSW) established a Data Analytics Centre (DAC) to facilitate data sharing between government entities and with the DAC.
Data.SA South Australian Government Data Directory	**South Australia** – Public Sector (Data Sharing) Act 2016 – authorises agencies to provide public sector data that they control to other public sector agencies for a wide arrange of purposes.
data.vic .gov.au VICTORIA	**Victoria** – Victorian Data Sharing Act 2017 – in December 2019 the Victorian government released for public consultation the recommendations from its review of the DataVic Access Policy. This review included a recommendation to release a new Open Data Policy to refocus on the purpose and benefits of the policy and the impact of open data.[13]
Queensland Government Queensland Government data	**Queensland** – The Queensland Open Data Policy Statement (September 2017) outlines the commitment to build a trusted data ecosystem that makes important data open for anyone to access, use and share. Queensland has created a Data Sharing and Analysis Office for inter-governmental data sharing.
data.wa.gov.au Providing access to WA government data	**Western Australia** – In August 2019 WA issued a discussion paper on privacy and responsible information sharing for the Western Australian public sector.[14] Currently Western Australia operates with a Whole of Government Open Data Policy (April 2015) that aims to improve management and use of the WA public sector's data assets.
Tasmanian Government	**Tasmania** has introduced an information sharing arrangement called the Administrative Data Exchange Protocol for Tasmania (ADEPT). ADEPT is intended to encourage an organisational culture in which information collected and held by government is valued and managed as an asset.
ACT data.act.gov.au	**The Territories** are yet to implement specific legislation on data sharing. **ACT** – Proactive Release of Data (Open Data) Policy 2015 [15] – the ACT provides an open data portal that provides data for a variety of specific use cases.

7. Department of Prime Minister and Cabinet, The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry, 2018. Refer https://dataavailability.pmc.gov.au/sites/default/files/govt-responsepc-dau-inquiry.pdf
8. Australian Government, Department of the Prime Minister and Cabinet, Data Sharing and Release, Legislative Reforms, Discussion Paper, September 2019. Refer https://pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation
9. A Deloitte Access Economics study estimated the potential economic impact for Australia at up to $25 billion annually
10. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 69
11. Deloitte Center for Government Insights, How CDOs can overcome obstacles to open data sharing, 2019
12. Deloitte Center for Government Insights, How CDOs can overcome obstacles to open data sharing, 2019
13. Victorian Government, Department of Premier and Cabinet, DataVic Access Policy: Review and Recommendations, December 2019. Refer https://engage.vic.gov.au/open-data-policy-update
14. Western Australian Government, Privacy and Responsible Information Sharing for the Western Australian public sector: Discussion Paper, 2019. Refer https://www.wa.gov.au/sites/default/files/2019-08/Discussion%20paper_Privacy%20and%20Responsible%20Information%20Sharing.pdf
15. Capital Territory Government, Office of the Chief Digital Officer, Proactive Release of Data (Open Data) Policy, December 2015. Refer http://www.cmd.act.gov.au/__data/assets/pdf_file/0011/859430/2016-Proactive-Release-of-Data-Open-Data-Policy.pdf

It's time to pivot

It's time for the response of all levels of government to open data to pivot.

In both the public and private sectors, data-sharing is likely to evolve as:

- Citizen and consumer demand for transparency increases
- Regulatory changes require greater data sharing and move towards making public sector data 'open by default'
- Technology continues to change
- Businesses and governments identify new use cases and value that can be created from open data, and
- Citizens and consumers become more aware of the potential benefits of open data to them.

One of the objectives of the federal DATA legislation is to "move the paradigm from one which restricts access to data to one which authorises sharing and release when appropriate data safeguards are in place."[16]

The discussion paper noted calls for a national data system, the development of at least a consistent approach to data sharing, Data Sharing Principles to reduce the complexity which hinder the use of data, and greater alignment and standardisation of data sharing arrangements across and between federal, state, territory and local governments.[17]

Open Data Participants

Governments collect vast amounts of data on everything from health care, housing, and education to domestic and national security – both directly and through non-profits that they support. Governments also produce data, such as census data, labour information, financial market information, weather data, and global positioning system (GPS) data to name just a few.[18]

Government organisations participate in open data as data custodians (data holders) or as accredited users (data recipients). In addition entities can be designated as Accredited Data Service Providers.

Data Custodians

Data custodians are government organisations (including companies) who collect data for any purpose. Data custodians face two broad decisions about their data.

The first decision is about the nature of the data they share or release. It can be:

- Raw data – the primary data collected by the organisation
- Value-added data – data transformed by the application of insight or analysis
- Enhanced data – the sorting and integration of different data sets, including, for example the addition of third party data sets.

The PC report recommended that datasets which would be likely to generate significant additional community-wide net benefits beyond those obtained by the original data holder be designated as National Interest Datasets (NID).[19] Designation of a dataset as a NID would achieve wider sharing, use, and where appropriate, release by:[20]

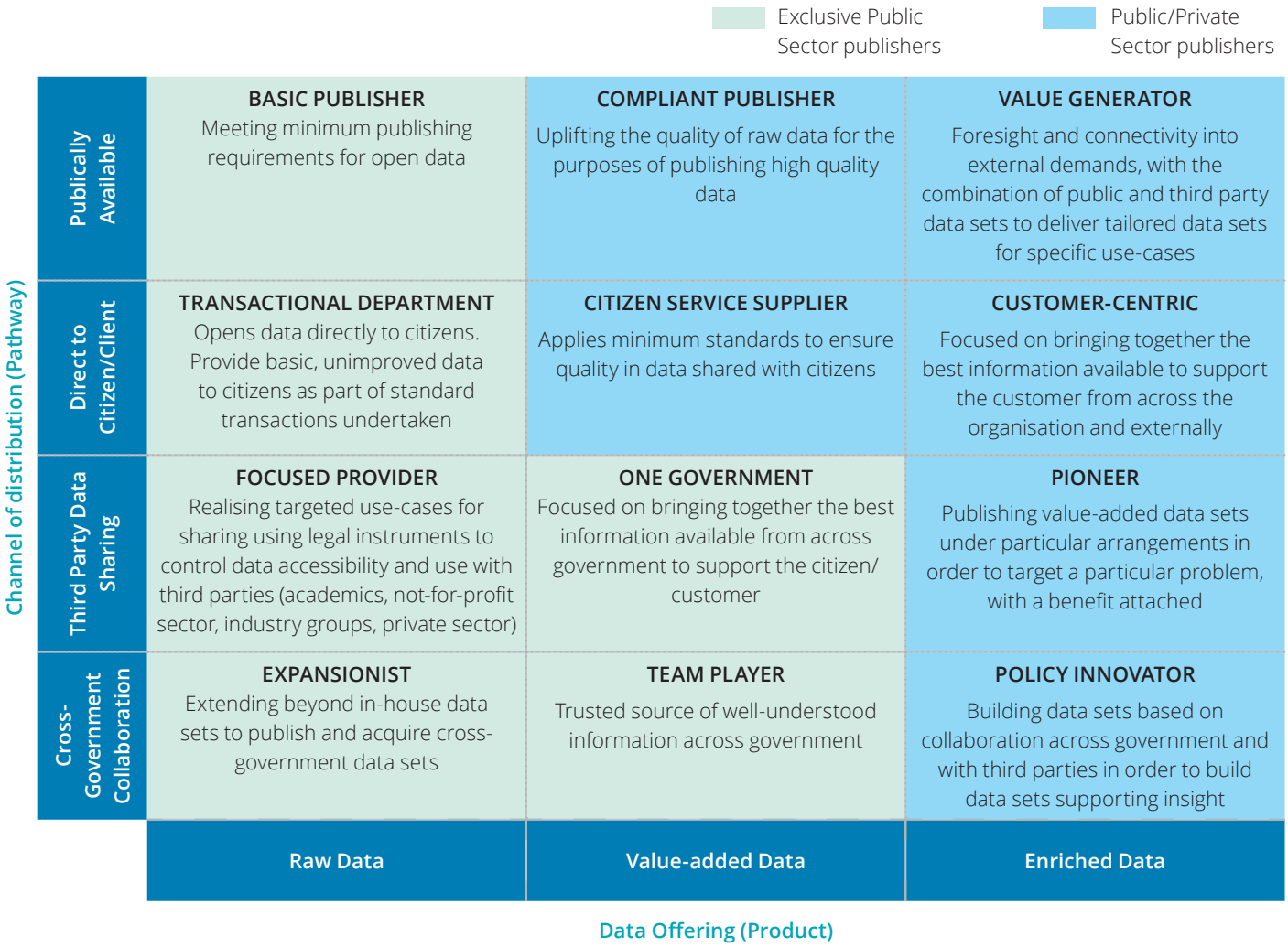
- Providing sufficient and predictable funding for data curation and updating
- Aggregating jurisdictionally-separated datasets
- Providing a framework in which to better link datasets across sectors and fields of endeavour.

The second decision for data custodians is about with whom each type of data is shared:

- Cross-government – data is shared with other government organisations
- Accredited third parties – trusted users from both the public and the private sector, for example research organisations and accredited private sector organisations, with whom data is shared for a limited purpose and with limitations on the ability of the accredited third parties to on-share the data they have received
- Citizens – government organisations could share information about a citizen with that citizen, or at the citizen's request, with an accredited third party nominated by the citizen
- Everyone – once shared, non-sensitive publicly funded data which is fully 'open' can be freely used, re-used and re-distributed by anyone.

These decisions result in a range of non-mutually exclusive options for government organisations to apply to the data sets they collect and hold.

16. Australian Government, Department of the Prime Minister and Cabinet, New Australian Government Data Sharing and Release Legislation: Issues Paper for Consultation, July 2018
17. Australian Government, Discussion paper, September 2019, page 8
18. Deloitte Center for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019, p2
19. Productivity Commission, Data Availability and Use, Recommendation 7.2 page 45
20. Productivity Commission, Data Availability and Use, page 24



Looking at open data through this frame avoids the binary "all or nothing" approach to data sharing that has often been used for open data discussions in government. This type of thinking takes off the table options that could provide much of the benefit of data sharing, but at less cost and/or lower risk.[21]

These decisions will be guided by the five Data Sharing Principles[22] which provide a way of sharing data that achieves the policy objectives in a safe and controlled manner:

Risk Area	Data Sharing Principles	Example Questions
Project	Data sharing is for an appropriate project or program of work	• Is the project in the public interest and does it satisfy a purpose test? • Are there any restrictions on how the shared data may be used?
People	Data is only available to authorised users	• Who is accessing the data? • What, if any, process for authorisation is required for people or organisations to access data?
Setting	The environment in which the data is shared minimises the risk of unauthorised use or disclosure	• Does the access environment prevent unauthorised use? • What IT security needs to be in place?
Data	Appropriate protections are applied to the data	• What further data treatment will be appropriate? • Can the data disclose identity?
Outputs	Outputs are appropriate for further sharing or release	• Will the output be released publicly? • Does the output adequately protect privacy and confidentiality? • Are the statistical results non-disclosive?

21. Deloitte Center for Government Insights, How CDOs can overcome obstacles to open data-sharing, 2019, p2
22. Australian Government, Department of the Prime Minster and Cabinet, Best Practice Guide to Applying Data Sharing Principles, 15 March 2019. Refer https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

One of the challenges for data custodians in the public sector is that public servants tasked with the role of compiling, licensing and publishing data have not always been trained in data governance practices. This in turn results in questions on data quality and a concomitant resistance to data sharing, both internally and externally. As a result, data custodians may choose to outsource the management of data request to an Accredited Data Service Provider.[23]

Accredited Users

Government organisations, as well as other organisations, can also be accredited users (data recipients). In addition to the opportunities that government organisations have as data holders, they have the ability to enhance the efficiency or effectiveness of the services they provide by ***receiving*** relevant data sets held by other organisations, particularly other government organisations. They can also use shared data they receive to enhance the evidence base to shape the design and implementation of government policy.

Under the proposals in the Data Sharing and Release discussion paper data custodians and accredited users will enter into a data sharing agreement to provide transparency on what data will be shared and how it will be used. However given one of the objectives is to remove barriers and streamline sharing and release of public sector data, it will be important that the mandatory terms developed for data sharing agreements do not introduce new actual or perceived barriers to sharing.[24]

Accredited Data Service Providers

The DS&R discussion paper notes that entities which have strong experience in data sharing and release – including data curation, data collation, linkage, and de-identification – could be accredited to act as intermediaries. These Accredited Data Service Providers (ADSPs) would aid others in sharing or releasing data to trusted users. ADSPs roles could also include data cleansing, secure data storage, and secure access to data sets. ADSPs may come from public, private and research sectors.[25] Examples of ADSPs could include the Australian Bureau of Statistics, and the Australian Institute of Health and Welfare.[26]

Impact Areas

Open data in government has the potential to have a significant positive impact on a government organisation. The DS&R discussion paper identified three primary purposes for which there was broad support for data sharing:[27]

- Improved policy and decision making – governments can leverage data to gain greater insights and formulate better policies[28, 29]
- Better services or improved quality of government service delivery informed by data sharing and release[30]
- Better and more coordinated research to drive improved social outcomes[31]

In addition, open data can bring a number of other benefits:

- Greater alignment with organisational purpose
- Improved risk management with data sharing contributing to better identification and understanding of risks, coordination of activities to mitigate risks, and improved resilience[32]
- Improved governance and enhanced transparency, resulting in more engaged and empowered citizens[33]
- Reduced cost of government service delivery – data can offer new ways to curb waste as well as to operate more efficiently and get more done with less[34]
- Exposure of government waste or corruption – with mounting public pressure for transparency and accountability, data can offer new ways to curb fraud and abuse[35, 36]
- Improved transparency as citizens, governments, industries and researchers use and share data, contributing to greater competition and innovation.[37]

Effective design and implementation by government organisations of their open data strategy will be important if government and society are to realise the benefits of open data sharing and release.

While there are pockets of excellence, data practices need to be improved across all departments. Transparent policies, processes and systems will be important to give people the confidence to move to a culture of 'responsibility to share' and 'open by default'. People will need to be educated in why open data in government is important and how to manage the risks. Adequate funding will be critical if open data if we are to meet the challenge set out in the PC report to transform the Australian society.

Increasingly, however, this potential is shadowed by a recognition that new technologies and data strategies come with a novel set of risks. If not approached carefully, innovative approaches to leveraging data can easily cause harm to individuals and communities and undermine trust.[38]

23. DPM&C (2018) page 18
24. DPM&C (September 2019), page 37
25. DPM&C (September 2019), page 44
26. DPM&C (2018) page 18
27. DPM&C (September 2019), page 21
28. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 113
29. Deloitte Center for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019, p1
30. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 111
31. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 115
32. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 110
33. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 111
34. Deloitte Center for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019, p1
35. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 114
36. Deloitte Center for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019, p1
37. Department of Prime Minister and Cabinet, Media Release, Greater competition will come from more access to data, 8 May 2017. See: https://ministers.pmc.gov.au/taylor/2017/greater-competition-will-come-more-access-data
38. Deloitte Center for Government Insights, Managing data ethics: a process-based approach for CDOs, 2019

The increase in the amount of data that is shared and the number of counter-parties with which this data is shared, where the data is sourced from systems that were not necessarily built with data sharing in mind, and shared via a new regulatory environment which introduces new obligations on data custodians and authorised data recipients together create a risk of unintended, and potentially unanticipated, adverse consequences. The increased sharing and release of information increases the risk of a data breach with the associated reputational costs for government organisations and personal costs for individuals.

In addition, some of the impacts of open data in government may be uncomfortable. It can invite external scrutiny on the efficacy of public policy. It can cause questions to be asked about the cost of certain programs.

As government organisations develop a more strategic response to open data there are a number of areas where they could be impacted that should be considered as part of the design of their open data strategy.

Strategic response – a strategic focus on the opportunities that open data in government provides, enables government organisations to use open data as a key element of delivering the policies, products or services embedded in their organisational purpose.

Citizen/Customer – sharing data between government departments can help organisations design better informed and more targeted policies to drive outcomes for citizens and customers as well as deliver more targeted and more effective services for citizens. The value of data is determined not by the data itself, but by the story it tells, the actions it empowers us to take and the outcomes this creates for citizens and customers.[39]

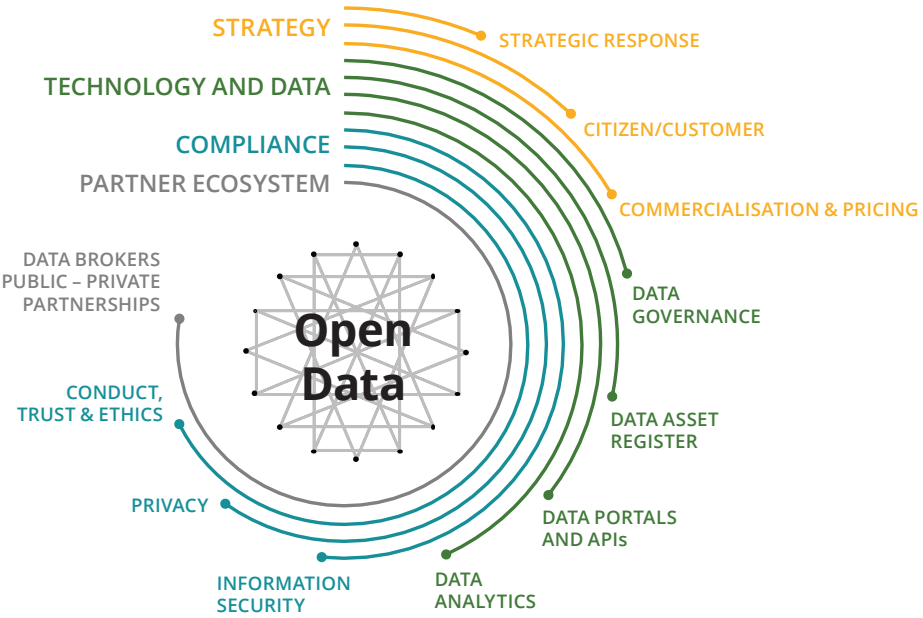
Commercialisation – governments around the world are considering the potential to publish raw high-value data sets via their portals, whilst adopting commercial models for value-added data streams.

Data Governance – designing and implementing the machinery for managing data throughout this ecosystem will require a considered and focussed approach. An organisation's Data Governance and Architecture (DG&A) capability needs to be able to respond to the compliance obligations of data sharing and open data legislation and rules.

Data Asset Registers – government organisations will need to have clearly identified the datasets that could be shared or released and have consistent standards to describe those data sets. Having established a data asset register, government organisations will also need to ensure there are processes in place to ensure the data is maintained and kept up-to-date.

Data Portals and APIs – a number of governments have established centralised data portals. Some government organisations have also created APIs to facilitate data sharing. Government organisations will need to identify which datasets will be released through a central data portal and which will be released through an API.

Data Analytics – governments increasingly rely on data-driven insights powered by algorithms.[40]



39. Deloitte, How CDOs can manage algorithmic risks, 2019
40. Deloitte, How CDOs can manage algorithmic risks, 2019

However data-driven policy is only as good as the data that drives it.

If technical capacities in government agencies are sub-optimal, poor data quality and reliability can produce worse policy than would have been created otherwise.[41]

With one of the outcomes of open data being greater sharing of data between government organisations, it will be important for a government organisation which is an accredited user to have the analytics capability to discover insights, solve challenges and expedite processes, and to have clear policies around the use of algorithms as part of its analytics capability.

Information Security – Cyber security is already one of the top three critical risks for almost all organisations. Greater release and sharing of data amplifies this risk. People understand that data can be used to improve lives but people are worried that information about them can fall into the wrong hands.[42]

It is easy for civil servants to overestimate the security measures taken to protect personal data when their technical capacities are limited or when they do not have a full overview of the vulnerabilities and threats that might be posed to that data or the individuals reflected in it.[43]

Privacy – Paradoxically, and spurred on by data issues in the private sector (notably Cambridge Analytica in a crowded field of corporate data breaches) and public sector (e.g. MyHealth's opt-out requirements), open data is resulting in an increased focus on privacy, consent and trust. As open data in government enables personal information to be shared between organisations, data privacy will become critical.[44]

For other data sets, consent will not have been obtained and de-identification of data sets will be critical. When de-identifying data, organisations need to consider the ***mosaic effect***, the phenomenon whereby it is possible to re-identify individuals in an anonymized data set by combining that data with external data sets. The trouble with this phenomenon is that it is never possible to know how advanced technologies for re-identification will become – they are consistently surprising experts with their effectiveness.[45]

Conduct, Trust and Ethics – The interest in and focus on data ethics is growing across the globe, in part in response to growing data literacy but also because of some high profile cases of abuse of data. Government organisations receiving data need to manage the risks introduced by using analytics and algorithms to assess that data. Although often enshrouded in an aura of objectivity and infallibility, algorithms can be vulnerable to a wide variety of risks, including accidental or intentional biases, errors, and fraud.[46] The increased use of data in policy-making and operations demand ethical engagement.[47] It raises questions about data ethics – how should we be using a data set, and even should we be using a data set?

Data ethics should be considered across governmental institutional processes and across different types of data, whether they target government efficiency or civic engagement. The most useful heuristic may be that ethical questions should be considered for every process in which data plays a role.[48]

Partner Ecosystem – as government organisations' use of open data expands, they are likely to create an eco-system of accredited data recipients with which they are sharing data, and organisations from whom they are receiving data. Government organisations will want to have a process to ensure that the privacy, information security and data ethics practices of organisations in their partner ecosystem do not expose them to reputational risk.

41. These were the two key messages from the roundtables undertaken by the Office of the National Data Commissioner to discuss the government's data reforms. Office of the National Data Commissioner, Building Trust through the data sharing principles, 19 March 2019. See: https://www.datacommissioner.gov.au/news/building-trust-through-data-sharing-principles
42. These were the two key messages from the roundtables undertaken by the Office of the National Data Commissioner to discuss the government's data reforms. Office of the National Data Commissioner, Building Trust through the data sharing principles, 19 March 2019. See: https://www.datacommissioner.gov.au/news/building-trust-through-data-sharing-principles
43. Deloitte Center for Government Insights, Managing data ethics: a process-based approach for CDOs, 2019
44. The consultation paper on the DS&R legislation noted that there are more than 500 existing data secrecy and confidentiality provisions across more than 175 different pieces of Australian Government legislation. The vast majority of these provisions prevent sharing of data, except in specific limited circumstances. (DPM&C (2018) p10) The Productivity Commission noted that 'while some may remain valid, they are rarely reviewed or modified. Many would no longer be fit for purpose.' (Productivity Commission, Finding 3.2 page133)
45. ASPE, "Minimizing disclosure risk in HHS open data initiatives," accessed January 8, 2019; Rich Murnane's Blog, "The 'mosaic effect," January 8, 2011
46. Deloitte, How CDOs can manage algorithmic risks, 2019
47. Deloitte Center for Government Insights, Managing data ethics: a process-based approach for CDOs, 2019
48. Deloitte Center for Government Insights, Managing data ethics: a process-based approach for CDOs, 2019

Ethics then and now

Traditional concepts	Ethics in a data context
Privacy has traditionally been understood as a possessive concept, in which information is intentionally shared or withheld.	Privacy is increasingly seen as transactional and collective, whereby access to personal information is granted on a differential basis in exchange for access to services and interactions online.
Prior and informed consent is the presumed condition for all use of an individual's personal data that is secured through research or medical processes. In effect, people must sign a form.	In the world of digital services, consent is often granted by individuals checking boxes on a Terms of Service form that they do not read. When large-scale data is collected from the internet or from administrative processes, without direct interaction with individuals, consent is rarely pursued. Informed consent seems, moreover, increasingly implausible, given an unpredictable digital context.
Sensitive data and personally identifiable information (PII) have traditionally been considered as discrete bits of information about individuals.	Sensitive data is increasingly understood to include novel types of data,[49] including data about interactions between individuals,[50] and some practitioners have also begun discussing community identifiable information.[51]
Data has traditionally been described as anonymous when all PII has been removed, and was thus understood as safe for public release.	Novel techniques for re-identifying individuals in anonymised data raise the question as to whether there is such a thing as anonymity in data.
There are several examples in the analog era of repurposing data for uses contrary to the intended ones, but this was largely a function of reinterpretation of findings.[52]	The advent of digital data sharing and duplication opens new opportunities for possible manipulation, repurposing, and reuse of data in ways that can directly contradict the actual original data and the individual's consent.

Key Questions

No matter what the level of maturity, all government organisations can progress their open data agenda.

Just as releasing data typically requires a rare combination of subject matter and technical expertise, so can figuring out which data sets to prioritise. Government officials cannot always predict what data sets, especially when used in concert with other data sets, might prove transformative.

> Government organisations sometimes do not have the management or technical bandwidth, or even the political strength, to release all of their agencies' data, even if this were always desirable. So prioritisation is key.[53]

As we move towards 'open by default' leaders in government organisations should be asking the following questions:

- Do we understand how open data in government could be used to help us achieve our organisational purpose?
- Can we better identify the citizens our activities are targeted at to help us achieve our organisational purpose efficiently and effectively?
- Do we understand where we are in our journey to open data maturity?
- Do we have a clear basis for understanding which data we should charge for and which should be truly open?
- Do we have the capabilities to curate and define data so that it is fit for sharing or release, particularly on an ongoing basis?
- Do we have an accurate data asset register which can be used to identify and prioritise data sets for sharing and release?
- Do we have a technology strategy to help us decide which data sets should be provided through shared portals and which should be provided through APIs?
- Do we have the ability to analyse our data sets and those we receive from other government departments or third parties to drive insights and decision making in our organisation? What is the governance structure of overseeing the risks emanating from algorithms?
- Is our information security environment robust?

49. Acxiom, "Defining 'sensitive' in world of consumer data," July 27, 2015; Safecredit, "Home"
50. See Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, "Evaluating the privacy properties of telephone metadata," PNAS, May 16, 2016
51. See UN OCHA, "Humanitarianism in the age of cyber-warfare," p.6, October 2014
52. For example, research on vulnerable populations (on substance abuse and violence among Australian aboriginals in the '80s and gay men in the United States in the '90s) has been leveraged to promote discriminatory legislation
53. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 53

- Do we have robust and timely processes for assessing privacy and confidentiality of data, particularly in an 'open by default' environment?
- Do our data ethics encourage trust by citizens in the way we handle data which we collect?
- Have we focused on the 'soft' capabilities required to assess ethical risks, conduct threat assessments and anticipate how constituents will experience data-driven processes as well as the 'hard technical capabilities relating to technology and data?
- Are we ready to embrace a broad eco-system of parties with whom data is shared?
- Do we have the capability to work with other parties to strengthen the reliability of data that we receive so that in turn we can strengthen the reliability of the data we share or release?

Last word

As the Productivity Commission noted "[I]n a world increasingly making use of the data of *others*, the primary unaddressed question should be: for how long will the public – the source of most of this information – trust a structure in which their actual rights are mainly limited to privacy?"[54]

Whether driven by societal expectations, government policies or legislation, the move towards an open data economy will result in increasing expectations that government data is 'open by default'.

Whether embraced because of its ability to enhance the delivery or a government organisation's purpose, or merely adopted to meet a compliance obligation, transitioning to an 'open by default' mindset and culture has the potential to require changes in organisations strategies, technology and data, compliance processes and the eco-system in which government operates.

In the longer term, open data in government has the potential to contribute to a more radical transformation of how government services are delivered.

The journey to 'open by default' presents both opportunities and challenges.

The time to take the next step to unlock government data is now.

54. Productivity Commission, Data Availability and Use, Report No 82, Canberra, March 2017, page 53

Contacts

Helena Hamilton
Partner, Data
+61 3 9671 6323
helenahamilton@deloitte.com.au

Stuart McCusker
Director, Data
+61 3 9671 6950
smccusker@deloitte.com.au

Kylie Watson
Partner, Risk
+61 2 6263 7450
kywatson@deloitte.com.au

Deanna Gibbs
Director, Risk
+61 2 6263 7595
degibbs@deloitte.com.au

Marion Burchell
Director, Strategy
+61 8 93657841
mburchell@deloitte.com.au

Ben Wylie
Partner, Technology
+61 3 9671 7681
bwylie@deloitte.com.au

Vinod Ralh
Director, Technology Platforms
+61 2 8260 6294
vralh@deloitte.com.au

Danielle Kafouris
Partner, Privacy
+61 3 9671 7658
dakafouris@deloitte.com.au

Paul Wiebusch
Partner, Open Data
+61 3 9671 7080
pwiebusch@deloitte.com.au

Ellen Derrick
Partner, Public Sector Leader
+61 2 6263 7069
ederrick@deloitte.com.au

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte
Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

About Deloitte Asia Pacific
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

About Deloitte Australia
In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2020 Deloitte Touche Tohmatsu.

Designed by CoRe Creative Services. RITM0372332