Data Use and Data Sharing in Government
New Regulations, Models and Challenges[1]

Peter Leonard[2]
Principal, Data Synergies
Professor of Practice, UNSW Business School

- *policy development, delivery of services, business applications and compliance: what's acceptable and what isn't*
- *algorithmic decision-making and government AI post Robodebt*
- *processes and tools for good data governance and data linkage projects*
- *what's covered and what's not*
- *Commonwealth, State and Territory data sharing laws: devils in the details*

Parliaments around the globe are legislating to facilitate shared uses and applications of data collected by government agencies through their respective interactions with citizens.

In countries with democratic traditions, and with data protection law developed from the family of the OECD Privacy Principles and U.S. Fair Information Principles, sharing of personal information about individual citizens is subject to statutory constraints, including through:

- purpose limitations in the enabling statute for a particular government agency, and
- operation of the data protection statute and subordinate regulatory instruments, and in particular the Collection Limitation Principle (*there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject*).

Use by decision makers in government agencies of outputs of data analytics activities are also often subject to administrative law and review requirements. In Australia, typically these include an obligation upon an administrative decision maker - usually assumed by the administrative law statute to be human - to evaluate the circumstances of the individual

[1] Copyright © Peter Leonard, Data Synergies 2020

[2] Peter Leonard is a data, content and technology business consultant and lawyer advising data-driven business and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (IT Systems and Management, and Business and Taxation Law). Peter chairs the IoTAA's Data Access, Use and Privacy work stream, the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of corporate and advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. The views expressed in this review report are those of the author not those of any of those other bodies and organisations.

case, to take into account all relevant considerations, to disregard irrelevant considerations, and (in many cases) to give reasons.

In short, administrative law usually has the effect of requiring there to be a human that:

- evaluates any data outputs that are inputs to a human decision-making process of deterministic reasoning to outcome;
- makes a decision having regard to all relevant considerations, and not only those that are reflected in data outputs.

In many jurisdictions, in addition to common law and statutory rights of judicial review the law confers upon affected individuals the right to seek other remedies such as a rights to review by an appeal authority or tribunal, a right to make a freedom of information request, a right of access to personal information about the individual, and so on.

Capabilities of artificial intelligence and machine learning (**AI/ML**) and advanced data analytics, particularly as enabled through linkage of multiple data sets across multiple government agencies, challenge the adequacy of conventional legal rights and remedies.

Humans applying deterministic reasoning may be aided by automated (machine enabled) sort, ranking, ranking or scoring using algorithmic techniques that are inherently probabilistic. Probabilistic outputs from application of well-designed and trained algorithms may be statistically reliable across a large cohort, but will likely remain unreliable in some cases, and particularly ‘at the ends of the Bell curve’.

A statute empowering a decision may not legally accommodate a machine aid that affects the criteria presented to the decision maker on which that human’s decision is made.

A fully automated outcome, without a ‘human in the loop’, may not be a defensible decision at all, particularly if deterministic reasoning was not applied to the particular case at any part of the decision tree.

In some cases, an outcome may not be explicable, and accordingly reasons cannot be proffered, particularly if ‘black box’ machine processing is not designed to be sufficiently transparent and therefore accountable.

Or the problem may be more straightforward: the input data is insufficient, biased or otherwise unrepresentative and therefore unreliable, or the outputs of deployment and use of AI/ML or other advanced data analytics have not been properly impact assessed, designed and managed.

The result may be that:

- inherent limitations as to suitability and reliability of machine outputs as an aid to human decision making will not have been properly and critically evaluated, or
- exposures of the process to legal challenge have not been considered and addressed, leaving a process and decision emanating from that process which is flawed and not capable of being sustained.

There are many things that can go wrong in applied data science. Every jurisdiction over recent years presents at least one exemplar villain to illustrate this proposition.

In Australia, our exemplar villain is *Robodebt*. *Robodebt #1* was a villain in data science methodology, in implementation (translation of data outputs into outcomes), and in failure to promptly review and re-assess following adverse feedback.

Other impediments to good data science include poor data quality and lack of standardisation of data sets, resulting both in poor data discoverability and limited depth and range of data that is ready for data linkage and analytics, and limited managerial skills and understanding of how to test the promise of the data science to effect social beneficence. AI/ML and other advanced data analytics may be deployed well, poorly, or somewhere in the middle. Properly considered and managed implementations of advanced data analytics and AI have demonstrated capability to reduce cost of delivery of government services, to enable services to be better targeted to areas of greatest need, and to improve citizens' interactions with government agencies. Poor implementations will erode digital trust, making it more difficult for government agencies in the future seeking to do things that are perceived by citizens as analogous to failed deployments.

Robodebt #2, anyone?

Data analytics can be difficult to promote within government agencies. Sometimes the concern of a data custodian within a government agency will be that permitting data sharing will lead to loss of their control of data, with unpredictable or undesirable risks or consequences. These concerns may or may not be clearly articulated, or related to social beneficence. For example:

- surgeons, operating room staff and hospitals may not welcome standardised outcomes based comparison of the incidence of complications, and comparison of reports by patients as to outcomes, of surgical procedures or other treatments conducted on patients with like symptoms and like pre-exiting co-morbidities undertaking like procedures or treatments in reasonably comparable facilities,
- government departments may not welcome quantitative outcome measurements that justify Treasury or Finance to cut their budgets,
- schools and teachers may not welcome properly standardised comparison of student cohorts that may measure effectiveness of individual teachers and schools.

Notwithstanding the many challenges in applied data science, the trajectory is clear:

- more government agencies undertaking more data sharing and linkage,
- more complex analytics,
- more machine enabled outputs, and
- an increasing diversity in outcomes affecting humans and the environment that are significantly influenced, if not driven, by machine outputs.

And this is the position even before pure AI/ML comes into play.

Factors driving this trajectory include:

- Citizens are demanding greater ease in dealing with government, including 'ask me once' and single point of entry for a range of government services.
- Most people want better targeted infrastructure, lower costs in delivery of infrastructure and services, less fraud and wastage, and so on.
- Good and respectful data analytics can address incidence of otherwise intractable areas of criminality and social and health disadvantage, including reduction of initial offending and re-offending in child abuse and domestic violence and targeting of community services towards at-risk individuals.
- Services that require a high degree of teaming across disparate service providers, such as disability and in-home healthcare services, can be targeted and delivered much more economically through good and respectful data analytics.
- Treasury and Finance want greater efficiencies and less staff within government agencies, and for government agencies to demonstrate delivery of value-for-money by matching of budget against measurable outcomes.
- Australian government agencies are unusually able to derive efficiencies through data linkage and sharing because key data sets are concentrated at only two levels of government, being Federal or State and Territory (with States and Territories having power to cause local government agencies to deal with data as the relevant State or Territory directs). Contrast many overseas jurisdictions, where health, education, police, taxation and other key data sets are controlled by different agencies and at multiple levels of government, leading to difficulties in achieving data linkage and integration.

We have talked about outcomes informed policy making for years. We finally have the tools to do it, when we have the courage to use them. Often this will require bringing onboard, or staring down, stakeholders that don't wish their performance to be measured. But the course is set.

Clearly, we will see more and more data linkage and data sharing by government agencies.

Why do we need data sharing statutes?

The first question to be asked about data sharing statutes might reasonably be: *why do we need them at all*? What is deficient in the existing combination of data privacy laws and administrative law remedies?

- **Individuation without disclosure and use of personal information**

Firstly, many forms of data sharing are not closely regulated by data privacy law, yet may still enable creation of outputs that can be used to effect individuated (differentiated) outcomes upon individuals or small cohorts of individuals.

That outcome might be any of denial of offer of a service, a different price for a service, withdrawal of a service, a demand for payment or reimbursement, an investigation or enforcement action.

Such outcomes may be particularly problematic in jurisdictions without broadly based human rights laws upon which these outcomes may be challenged. These outcomes may not constitute illegal discrimination, but still be regarded by many citizens and civil society organisations as unfair, unethical or otherwise unduly intrusive or socially undesirable.

How can such individuated outcomes be achieved without contravening the purpose limitation and without disclosure or handling of personal information about the affected individual?

Applying the commonly accepted view of most Australian general data privacy statutes:

- if personal information about an individual is reliably and verifiably deidentified (applying the current Australian usage of deidentification as substantively the same as pseudonymisation, subject to the following) in the sense that it is pseudonymised before the pseudonymised data set is provided to the data analytics services provider), that pseudonymisation is not be a use relevantly regulated by data privacy law (again, subject to the following), and
- the data analytics services provider implements technical, operational and legal safeguards against re-identification, so that the risk of re-identification of any individual from data handling by the data analytics services provider is demonstrably and reliably remote, and
- the data analytics services provider does not disclose that pseudonymised data or other outputs to anyone else in a form that any entity (whether the direct recipient or another downstream entity) receiving that data could re-identify an individual (using whatever other information that is available to that recipient entity),
  <u>then</u>
- the output may be used to the recipient entity to effect a differentiated and individualised outcome upon an affected individual (who may have been the data subject of the data used to create that output, or may be 'a look-alike' to a data subject), without operation of the data privacy statute's purpose limitation, or any requirement of notice to, or consent of, the affected individual.

Most Australia data protection statutes today do not address such individuated outcomes. Contrast the position under the EU *General Data Protection Regulation* (**GDPR**), where Article 22 *(Automated individual decision-making, including profiling)* operates to require a data subject's explicit consent where such an application involves automated individual decision making, even if data is reliably and verifiably managed as pseudonymised data as above described.

Contrast also the position in jurisdictions, such as Canada, that have implemented requirements for algorithmic accountability by government agencies.

- **Challenges of notice and consent**

Many applications of AI/ML and other advanced data analytics proposed by government agencies today <u>do</u> involve disclosure or handling of personal information in ways that activate the data privacy statute's purpose limitation and requirements of notice to, or consent of, the affected individual. This requirement of notice (and sometimes consent) should extend to statement of the nature and purpose of and from the particular handling act or practice, and therefore possible outcomes.

As already noted, typical data privacy laws in advanced democracies limit activities of regulated agencies in collection, disclosure and subsequent use of personal information about an individual, principally through combined operation of a 'purpose limitation' and requirements as to notice and consent. Generally under these statutes, if an entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), as disclosed by notice and sometimes requiring consent (i.e. for collection and handling of sensitive personal information, such as health information about an individual), the entity must not use or disclose the information for another purpose (the secondary purpose), unless the secondary purpose is directly related to the primary purpose, or an affected individual has provided fully informed and voluntary consent.

However, 'consent' is often not an appropriate threshold for dealings by citizens with government. Many dealings by citizens with government are not fully voluntary, and accordingly 'consent' does not have the necessary element of choice and voluntariness. In any event, consent often will not have been sought and obtained upfront for applications of data sharing between government agencies because those applications will not have been understood at the time of collection. Consenting as to already collected data, or 're-consenting', is sometimes possible, but often practically problematic.

Exceptions to data privacy laws

Typical data privacy laws include exceptions to the 'purpose limitation' and requirements as to notice and consent, which exceptions permit specific secondary disclosures and uses of personal information about individuals.

Specific exceptions vary significantly by statute, but often exceptions will include concepts such as:

- as required or authorised by or under a law or an order of a court or statutory tribunal,
- to prevent or lessen a serious and imminent threat to the life or health of an individual,
- for scientific and medical research, often conditioned upon compliance with particular guidelines or other regulatory requirements as to the management of the research project.

Often any non-specific statutory exception to the effect of 'as required or authorised by or under a law' will be of limited practical utility for data linkage projects, as the relevant secondary handling will not meet the standard (however it is expressed in the particular statute) 'as required or authorised by or under a law'.

Some statutes empower the Privacy Commissioner or another regulatory authority to issue a direction which has the effect of overriding the data privacy statute for a limited use case. New South Wales examples includes the NSW Privacy Commissioner's *Direction for Domestic Violence Disclosure Scheme pilot*, and *Direction under s. 41(1) of the Privacy and Personal Information Protection Act 1998 in relation to Youth on Track.*

Other statutes do not relevantly empower the regulatory authority to override the operation of the data privacy statute, but the regulator instead provides guidance as to application of the statute. Federal examples include the Office of the Australian Information Commissioner's *Guidelines on Data Matching in Australian Government Administration*, June 2014, the OAIC's *Guide to data analytics and the Australian Privacy Principles*, March 2018, the OAIC's *De-identification and the Privacy Act*, March 2018, and the Department of Prime Minister and Cabinet's *Best Practice Guide to Applying Data Sharing Principles*, March 2019.

Some statutes include provisions which override the general data privacy statute and specifically enable anticipated disclosures for secondary uses of particular databases. These enabling provisions can be quite controversial, particularly when sensitive data sets such as personal health data is involved. Concerns as to secondary uses permitted by the *My Health Records Act* 2012 (C'th) ultimately led to passage of the *My Health Records Amendment (Strengthening Privacy) Act* 2018. The first Australian primary health care data linkage project started in Western Australia in 2007, when Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data were linked to several state health care datasets. (It is interesting to note in passing that the two Australian States which do not have comprehensive health data privacy laws, being Western Australia and South Australia, were earliest States to progress data linkage initiatives that involve State health data sets.) Since then there have been various Federal statutory enactments which have enabled use of MBS or PBS data for a range of non-research purposes, most recently for detection and investigating fraudulent claims: see the *Health Legislation Amendment (Data-Matching and Other Matters) Act 2019*.

To summarise:

- Data privacy laws are one hurdle to data sharing between government agencies.
- Citizen consent is already not required for a range of data matching activities conducted by government agencies, including health and medical research conducted using the limited research exception from the federal Privacy Act 1988.
- Various other statutory overrides of Federal, State and Territory data privacy statutes enable specific data sharing activities without citizen consent.
- In any event, consent is often a concept of limited practical utility when citizens deal with government: often a citizen will face a choice of providing 'consent' to obtain a government service or benefit, or not getting that service or benefit. Many purported 'consents' required by government agencies fail the test of a fair informed consent.

Other constraints on data sharing and secondary uses by government agencies

In addition to requirements of relevant information privacy statutes, many government agencies and business enterprises considering data linkage projects or data sharing must address other legal or contractual constraints.

These constraints may be:

- specific statutory prohibitions on sharing,
- specific statutory prohibitions on use of data even where reliably and pervasively de-identified,
- contractual restrictions as to sharing, including conditions in contractual licences,
- copyright restrictions,
- a duty of confidence either stated or implied by the content of the information, or because the information was collected in circumstances where confidentiality is expected – e.g. medical records and bank customer records,
- sector or industry-specific regulation or guidance about handling individuals' information, including industry sector codes of practice.

Most government agencies (other than government departments headed by a Minister) derive their powers entirely from statute or regulation. The relevant legislation often defines the organisation's functions in terms of its purposes, the things that it must do and the things that it may do, and the powers which the organisation may exercise in order to achieve those purposes. It will generally be necessary to identify where the data sharing in question would fit, if at all, into the range of things that the organisation is able to do. Broadly, there are three ways in which it may do so:

- express obligations – occasionally, a government agency will be legally obliged to share particular information with a named organisation.
- express powers – sometimes, a government agency will have an express power to share information, usually only for certain purposes.
- implied powers – often, the legislation regulating a government agency's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted.

Sometimes an enabling statute will simply not allow use of particular data outside a specific function of a specific agency.

Or, an enabling statute won't have addressed the issue at all, leaving significant uncertainty as to what is the extent of data sharing that is permitted.

Data sharing statutes generally

Data sharing statutes legally facilitate data sharing and data linkage projects under defined conditions (such as following impact assessment and implementation of technical, operational, contractual and other controls and safeguards) using data sets controlled by different Government agencies within the relevant jurisdiction of that statute.

Three states have data sharing statutes: in order of their enactment (from oldest to youngest) NSW, South Australia and Victoria. The relevant statutes are:

- NSW: *Data Sharing (Government Sector) Act* 2015,
- South Australia: *Public Sector (Data Sharing) Act* 2016, and
- Victoria: *Victorian Data Sharing Act* 2017.

Western Australia recently completed a consultation as to a proposed data sharing statute, but as at March 2020 had not announced the outcome of that consultation.

The common permissive element of data sharing statutes is overriding limitations imposed by earlier statutes as to how relevant state government agencies may use and share data, subject to any further limiting conditions as defined in the relevant data sharing act.

Divergences between state statutes include:

- the extent to which the statutes override relevant state information privacy or health data privacy statutes in relation to data inputs provided to the authorised data analytics authority, and
- the extent of jurisdiction and control of the state privacy/information commissioner in relation to uses and disclosures of personal information, being information about individuals that are reasonably identifiable by any recipient of relevant information, whether or not the subject individual is identifiable to the data discloser.

The NSW *Data Sharing (Government Sector) Act* 2015 was the first of the Australian State data sharing statutes. Gaps and limitations in the NSW Act reflect its comparative age: four years is a long time in applied data science.

The NSW Act does not limit the operation of the NSW data privacy statutes in any relevant way, or override the jurisdiction of the NSW Privacy Commissioner in her administration of those statutes: section 12. Nothing in the Act permits or requires the DAC or another government sector agency to collect, use, disclose, protect, keep, retain or dispose of any government sector data that is health information or personal information except in compliance with the privacy legislation. However, the Privacy Commissioner has facilitated limited, controlled and safeguarded data linkage: see for example the NSW Privacy Commissioner *Direction under s. 41(1) of the Privacy and Personal Information Protection Act 1998 in relation to "Their Futures Matter" Project*.

The NSW Act in *Part 3 Data sharing safeguards* includes high level provisions as to safeguards of data privacy, government confidentiality and commercial confidentiality, but no detail as to technical, operational and legal data governance and data management:

sections 11 to 15. The NSW Act does not address allocation and use of data linkage keys, or operation of a deidentification data linkage environment, and what would be reasonable controls and safeguards for operation of that environment. As a result, there can be contention as to what standards and requirements are appropriate for the NSW Data Analytics Centre (**DAC**) and that environment, and whether Federal guidance, or guidance in other States, should be applied in NSW. This leads to legal complexities when Multistate or State and Federal datasets are proposed to be linked.

The DAC is authorised to share with the source government sector agencies the results of data analytics work that it has carried out on data provided to it by a government sector agency under this Act, but is not authorised to share that data with any other agency, person or body: section 9.

The NSW Data Analytics Centre cannot call-in data for data sharing. The Minister may direct a government sector agency "in writing to provide specified government sector data that it controls to the DAC within 14 days or such longer period specified in the direction, but only if the Premier has advised the Minister that the data concerned is required to be shared for the purpose of advancing a Government policy": section 7(1).

The purposes for which government agencies may voluntarily authorise the DAC to undertake data linkage and data analytics work are significantly constrained:

- to enable data analytics work to be carried out on the data to identify issues and solutions regarding Government policy making, program management and service planning and delivery by the government sector agencies,
- to enable related government sector agencies (such as branches, offices and other agencies within or otherwise related to a Public Service agency) to develop better Government policy making, program management and service planning and delivery by the agencies, and
- such other purposes as may be prescribed by the regulations: section 6.

By contrast, the *Victorian Data Sharing Act* 2017 Act facilitates data sharing in the Victorian public sector for the purpose of informing broader government policymaking, service planning and design: section 5.

The Act establishes the statutory position of the chief data officer (**CDO**) who is the head of the Victorian Centre for Data Insights. The CDO may request data from data sharing bodies (such as departments, Victoria Police, public sector bodies and public entities), and designated bodies (such as commissions, integrity oversight bodies, local councils and courts). However, designated bodies are not required to respond to the request. The Act expressly authorises data sharing bodies and designated bodies to provide data containing personal and health information (identifiable data) to the CDO on the CDO's request, as well as to other data analytics bodies (departments and any other public sector agencies prescribed in the regulations): sections 15 and 16. As with the NSW Act, the Victorian Act overrides secrecy provisions in legislation that may otherwise prevent agencies sharing data.

Importantly, section 16 of the Victorian Act allows the sharing of identifiable data by data sharing bodies and designated bodies with the centre and data analytics bodies without an individual's consent and in circumstances where the sharing may not be otherwise permitted by the Victorian privacy legislation. To this extent, the Act limits the right to privacy. However, that limitation is subject to statutory protections, as follows:

> ***17 Chief Data Officer or data analytics body may use identifiable data for the purpose of data integration***
>
> *The Chief Data Officer or a data analytics body, in accordance with section 5, may collect, hold, manage and use identifiable data received from data sharing bodies and designated bodies under this Act for the purpose of data integration.*
>
> ***18 Restrictions on the use of identifiable data for the purpose of data analytics work***
>
> *(1) The Chief Data Officer or a data analytics body must take reasonable steps to ensure that data received from data sharing bodies and designated bodies under this Act no longer relates to an identifiable individual or an individual who can reasonably be identified before using that data for the purpose of data analytics work.*
>
> *(2) For the purposes of subsection (1), the Chief Data Officer or a data analytics body must have regard to the following—*
>
> *(a) the de-identification techniques applied to treat the data;*
>
> *(b) the technical and administrative safeguards and protections implemented in the data analytics environment to protect the privacy of individuals;*
>
> *(c) any other considerations specified in the guidelines issued by the Chief Data Officer.*
>
> ***19 Restriction on the disclosure of results of data analytics work***
>
> *Before disclosing the results of data analytics work, the Chief Data Officer or a data analytics body must ensure that the results to be disclosed include only de-identified data.*

The South Australian Act, similarly to the Victorian Act, is broadly permissive as to activities of the data analytics body, the Office for Data Analytics (**ODA**), including to enable data analytics work to be carried out on the data to identify issues and solutions regarding Government policy making, program management and service planning and delivery by public sector agencies: section 8.

The ODA may, with the written approval of the Minister, direct a public sector agency to provide public sector data to ODA for the purposes of carrying out its functions: section 6(4). The Minister responsible for the ODA also has broad powers to call-in data: section 9.

The South Australian Act goes significantly further than the NSW and Victorian Acts in permitting the ODA to make the results of that data analytics work available to public sector agencies, to the private sector and to the general public as ODA sees fit; section 6(2)(b).

The prescription of controls and safeguards to be followed by the data analytics body is in marked contrast to both the NSW and Victorian Acts. The Trusted Access Principles in section 7 of the South Australian Act derive from the Five Safes Framework (discussed further later in this paper) that will also underlie the proposed Federal data sharing statute, and accordingly are set out below in full:

> *7—**Trusted access principles***
>
> *(1) The trusted access principles to be applied in respect of the sharing and use of public sector data under this Act are set out in this section.*
>
> *(2) **Safe projects***
>
> *The purpose for which data is proposed to be shared and used must be assessed as appropriate having regard to—*
>
> > *(a) whether the data is necessary for the purpose; and*
> >
> > *(b) the proposed use of the data; and*
> >
> > *(c) whether the purpose for which data is proposed to be shared and used will be of value to the public; and*
> >
> > *(d) whether the public interest in the proposed sharing and use of data outweighs any contrary public interest; and*
> >
> > *(e) whether there is a risk of loss, harm or other detriment to the community if the sharing and use of the data does not occur.*
>
> *(3) **Safe people***
>
> *A proposed data recipient must be assessed as an appropriate public sector agency with whom data may be shared for a particular purpose having regard to—*
>
> > *(a) whether the proposed data recipient is appropriately equipped and in possession of the relevant skills and experience to effectively use data for the proposed purpose; and*
> >
> > *(b) whether the proposed data recipient will restrict access to the data to specified persons with appropriate security clearance; and*
> >
> > *(c) whether the data provider will be able to engage with the data recipient to support the use of the data for the purpose; and*
> >
> > *(d) whether other persons or bodies in addition to the data recipient are invested in the outputs of the project and the motivations of those persons or bodies to be so invested.*

*(4) **Safe data***

(a) If data to be shared and used contains personal information, the personal information must be de-identified unless—

(i) the person to whom the personal information relates has consented to the sharing and use; or

(ii) the sharing and use of the personal information is reasonably related to the original purpose for which it was collected and there is no reason to think that the person to whom the information relates would object to the sharing and use; or

(iii) the sharing and use of the personal information is in connection with a criminal investigation or criminal proceedings or proceedings for the imposition of a penalty; or

(iv) the sharing and use of the personal information is in connection with the wellbeing, welfare or protection of a child or children or other vulnerable person; or

(v) the sharing and use of the personal information is reasonably necessary to prevent or lessen a threat to the life, health or safety of a person; or

(vi) the purpose of the sharing and use of the personal information cannot be achieved through the use of de-identified data and it would be impracticable in the circumstances to seek the consent of the person to whom the information relates; or

(vii) the sharing and use of the personal information is for a prescribed purpose or occurs in prescribed circumstances;

(b) Data to be shared and used for a purpose must be assessed as appropriate for that purpose having regard to—

(i) whether the data is of the necessary quality for the proposed use (such as being accurate, relevant and timely); and

(ii) whether the data relates to people; and

(iii) if data containing personal information is to be de-identified, how that de-identification will be undertaken and whether the data may be re-identified, and if so, how it may be re-identified.

*(5) **Safe settings***

The environments in which the data will be stored, accessed and used must be assessed as appropriate having regard to—

(a) the physical location where the data will be stored and used; and

(b) the location of any linked data sets; and

(c) whether the proposed data recipient has appropriate security and technical safeguards in place to ensure data remains secure and not subject to unauthorised access and use (such as secure login, user authentication, encryption and supervision or surveillance); and

(d) the likelihood of deliberate or accidental disclosure or use occurring; and

(e) how the data will be dealt with after it has been used for the purpose for which it is shared.

(6) ***Safe outputs***

The publication or other disclosure of the results of data analytics work conducted on data shared under this Act must be assessed as appropriate having regard to—

(a) the nature of the proposed publication or disclosure; and

(b) who is the likely audience of the publication or disclosure; and

(c) the likelihood and extent to which the publication or disclosure may contribute to the identification of a person to whom the data relates; and

(d) whether the results of the data analytics work or other data for publication or disclosure will be audited and whether that process involves the data provider.

The South Australian ODA may disclosure personally identifying outputs, subject to compliance with the Trusted Data Principles, and in particular the Safe Outputs Principle in clause 7(6).

The principal constraint that is common to the NSW and Victorian Acts is that they do not permit disclosure of personally identifying data outputs from the data analytics activities conducted within the controlled and safeguarded data linkage environment. Accordingly, the prospective operation of information privacy and health data privacy statutes in NSW and Victoria, and the jurisdiction and control of the state privacy/information commissioner over uses and disclosures of personal information relating to identifiable individuals, remain important constraints in those States upon release of any personally identifying data outputs by the data linkage centre.

Federal (Commonwealth)

The *Privacy Act* 1988 (C'th) (**Federal Privacy Act**) is the principal privacy statute in Australia.

The Federal Privacy Act regulates collection, use, disclosure and retention by Federal Government agencies and many business enterprises of 'personal information' that is collected for inclusion in any form of print or electronic 'record' or in a 'generally available publication'. The key rules are set out as the Australian Privacy Principles (APPs).

The Australian Privacy Commissioner has some limited and circumscribed powers to approve particular forms of data sharing. These powers have been exercised in, for example, the *National Health (Privacy) Rules 2018*. The Federal Privacy Act has an important exception to the APPs that applies, in particular, to the Australian Institute of Health and Welfare: section 95 of the Act permits the AIHW to take actions that might otherwise breach an APP, if those actions are for medical research and in accordance with the *Guidelines under Section 95 of the Privacy Act 1988* issued by the National Health and Medical Research Council.

The *Data Availability and Use Inquiry Report* (May 2017) of the Productivity Commission concluded “that lack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia's data”.   The Productivity Commission stated that marginal changes to existing structures and legislation would not suffice and recommended reforms “aimed at moving from a system based on risk aversion and avoidance, to one based on transparency and confidence in data processes, treating data as an asset and not a threat”. Key proposals included for enactment of a federal Data Sharing and Release Act, and establishment a National Data Custodian to guide and monitor new access and use arrangements, including proactively managing risks and broader ethical considerations around data use.

The Australian Government’s response stated that greater access to public sector data with a consistent approach to managing risk can improve research solutions to current and emerging social, environmental and economic issues” and stated the Federal Government’s commitment to:

- establishing a National Data Commissioner to implement and oversee a simpler, more efficient data sharing and release framework.
- introducing legislation to improve the sharing, use and reuse of public sector data while maintaining the strong security and privacy protections the community expects.
- introducing a Consumer Data Right (**CDR**) to allow consumers to share their transaction, usage and product data with service competitors and comparison services.”

The data sharing and release bill, when drafted, will address the first two commitments.

The Bill is expected to be introduced into the Federal Parliament in Q2 2020, following extensive consultations with interested stakeholders that have informed development of policy and drafting of this Bill.

The most detailed statements to date (March 2020) as to the outcomes of those consultations have been the *Best Practice Guide to Applying Data Sharing Principles –March 2019* and Data Sharing and Release – Legislative Reforms Discussion Paper of September 2019. The next likely release may be an Exposure Draft of the bill, which media reports suggest will be entitled the *Data Availability and Transparency Bill* (or as an Act, the *DATA*, reflecting increasing Americanisation in selection of catchy acronyms for Australian statutes).

The Federal Data Sharing Principles will be based on the *Five Safes Framework* as developed in the United Kingdom at the Office of National Statistics and substantially developed by, among other bodies, a technical team at Australian Computer Society led by NSW's Chief Data Scientist, Dr Ian Oppermann. It remains to be seen how closely the restatement of the Five Safes Framework into the Federal Data Sharing Principles reflects the restatement of the Five Safes Framework into section 7 of the South Australian Act, as set out in full above. In any event, the five safes may be summarised as follows:

- Projects: Data is shared for an appropriate purpose that delivers a public benefit.
- People: The user has the appropriate authority to access the data.
- Settings: The environment in which the data is shared minimises the risk of unauthorised use or disclosure.
- Data: Appropriate and proportionate protections are applied to the data.
- Output: The output from the data sharing arrangement is appropriately safeguarded before any further sharing or release.

The aim is to enable a privacy-by-design approach to data sharing, by balancing the benefits of using government data with a range of risk-management controls and treatments (particularly those managing disclosure risks). By focusing on controls and benefits, instead of merely reducing the level of detail in data as shared, the Principles can assist with maximising the usefulness of the data.

The Federal Data Sharing Principles will not of themselves operate as an authorisation framework or an alternative to privacy impact assessment. Often a privacy impact assessment will be required to ensure that each stage in a data sharing environment is appropriately privacy and security engineered, through reliable and verifiable technical, operational and legal controls and safeguards that address how an isolated data linkage and data analytics environment is established and managed, and that mitigate risk of disclosure of personal information outside that isolated environment. The impact assessment should address:

- what is allowed into that environment (i.e. generally require that personal identifiers with which data sets are associated are replaced by transactor linkage keys before the data sets enter the environment),
- how the data linkage and analytics environment is managed, overseen and audited, and
- what is allowed out of that environment by way of reports, insights, or other outputs, and then subject to what conditions and controls, including as to availability and use.

A core element of responsible data analytics governance is management of the data analytics environment and what is allowed out of it. A baseline is a set of particular technical, operational and legal controls and safeguards that ensure that the five safes requirements are reliably (consistently) and verifiably applied.

Although relevant controls vary, there are typically five key control elements:

- separation of persons or entities with access to individual identifying information from those persons or entities ('trusted third parties') conducting analytics using data sets which have been pseudonymised,
- replacement of direct or indirect personal identifiers in the merged data sets with a linkage code, or transactor key, which enables the service provider to infer that an identifiable transactor found in each data set is a unique transactor, although not identifiable,
- a combination of technical, operational, contractual and otherwise legally enforceable safeguards which reliably and verifiably ensure that uses of data outputs are only in accordance with stated purposes, that individuals that are the subject of transaction data are not re-identified, and that records of personal information about those individuals held by any relevant party are not augmented or supplemented in any way through the controlled process,
- information governance oversight, data process controls, change control procedures and quality assurance processes that ensure that each of these things are reliably and verifiably implemented and then reliable in ongoing operation and that any change in data flows or deviation from required practices and procedures is promptly identified, considered and (if need be) addressed by appropriate risk mitigation measures, and
- controls over outputs.

The principal safeguard should be pseudonymisation wherever reasonably practicable and conduct of data analytics in controlled environments that facilitate privacy protective 'data linkage' of individual level data (i.e. transaction records) that is about individuals or individual entities through joining of data sets of individual level data using pseudonymised linkage (sometimes called pseudo-identifiers).

Outputs require particularly careful assessment, including to ensure:

- accountability for reliability of those outputs and the circumstances in which they may be used to effect outcomes, and
- mitigation of risks that any direct or indirect recipient of those outputs might be able to identify an individual from analysis of those outputs, including through further data matching or mosaic analysis using other data sets available to that recipient. If the risk of any such reidentification is assessed by the data custodian as greater than remote, the data custodian should be treat the output as personal information about any potentially reidentifiable individual, even if the data custodian could not itself identify the individual and the output appeared to be deidentified.

For the reasons discussed earlier in this paper, conventional data privacy analysis may not address how outputs might be used to infer characteristics of particular unidentifiable individuals or enable them to be treated differently from other individuals or otherwise unfairly.

Outputs will often be insights or reports that are designed to be at a level of aggregation that precludes reidentification of individuals or households within a cohort and that therefore cannot be used to effect outcomes that are individualised. Such outputs will be sufficient for many applications in development and administration of government policy.

The issues are more complex where outputs are disaggregated, particularly where outputs enable individuals to be rated or scored. Individualised outputs might be any of:

- a reverse look-up (de-pseudonymisation) capability or flag, that enables a particular person or entity to be differentiated in a large or small cohort for particular treatment,
- a list of attributes that can then be used to differentiate a single person or entity in a large or small cohort for particular treatment, or
- an algorithm which automates such differentiation to similar effect.

Such disaggregated and individualised outputs may be reasonably required to effect socially beneficial outcomes: for example, to manage of child abuse and domestic violence re-offending, and to identify at-risk individuals. However, such cases require careful impact assessment to ensure that the outcomes are fair, equitable and sufficiently transparent, and that there is appropriate accountability built into the translation of outputs to outcomes.

The current understanding is that the Federal DATA Bill will effect controls over outcomes by precluding use of the DATA data sharing enablement framework (at least, of itself) for enforcement or compliance activities. Such activities would require separate and specific statutory authorisation, an example of which is the health benefits fraud detection and enforcement enablement framework established by the *Health Legislation Amendment (Data-Matching and Other Matters) Act 2019*). The DATA is not anticipated to include broader requirements as to adoption of algorithmic accountability measures, although the Data Sharing Principles (in particular, as to impact assessment and Safe Outputs) include important elements that are common in algorithmic accountability proposals and some adopted accountability frameworks (such as the Canadian model).

Conclusions

Data linkage and data sharing activities by government agencies throughout Australia will continue to rapidly grow.

Well drafted and managed data sharing statutes play an important role in facilitating controlled and safeguarded data linkage and data sharing and supplement, but should not supplant, data privacy laws and administrative law.

Data sharing statutes do not however address important emerging issues, such as algorithmic individuation and whether a citizen should have a legislated right to inferences about them being fair and reasonable. The broader questions of acceptable bounds to government algorithmically driven activities are with scope of a number of ongoing reviews, including the Australian Human Rights and Equal Opportunity Commission's Technology Rights Project.   As these important societal questions gain traction in media and public policy debates, there is a significant risk that reasoned discussion about data linkage within government to create controlled and restricted outputs is confused with debate as to how to ensure that uses of analytics or behavioural nudges by governments to effect outcomes are fair, equitable, accountable and transparent.

Peter Leonard

8 March 2020

Appendix: a primer on data privacy in New South Wales

The NSW Privacy Commissioner oversees two main privacy laws, being:

- the Privacy and Personal Information Protection Act 1998 (**PPIP Act**), and
- the Health Records Information Privacy Act 2002 (**HRIP Act**)

The PPIP Act and HRIP Act provide for the proper collection, holding, security, access to, amendment, disposal, use and disclosure of personal and health information.

The PPIP Act provides this through 12 Information Protection Principles (**IPPs**).

The HRIP Act provides 15 Health Privacy Principles (**HPPs**).

In addition to the HPPs, private sector persons must comply with other HRIP Act provisions relating to retention, access and amendment of health information, as per Part 4 of the HRIP Act.

NSW public sector agencies are bound by both the PPIP Act and HRIP Act. Bound entities include:

- state government agencies,
- local councils,
- universities, and
- Ministers and Minister's offices,

but o=in the case of the PPIP Act do not include state owned corporations (**SOCs**), unless a SOC elects to follow the Act.

The HRIP Act applies to a broader range of entities, including:

- NSW public sector agencies, including local councils and universities,
- public and private sector health organisations such as private and public hospitals and medical centres,
- health service providers such as GPs, dentists, therapists, physiotherapists, chiropractors and optometrists, and
- businesses with an annual turnover of over $3 million that holds health information, such as insurance service providers.

The NSW Privacy Commissioner does not have privacy jurisdiction over the conduct of private sector persons (individuals, corporations, partnerships and trusts), except where they are bound by the HRIP Act.

The NSW Privacy Commissioner, with the approval of the Attorney General, may make a Public Interest Direction to waive or make changes to the requirements for a public sector agency to comply with an Information Protection Principle (IPP), or requirements for regulate entities to comply with a Health Privacy Principle (HPP).

A Privacy Code of Practice is a legal instrument which allows a public sector agency or organisation to make changes to A Privacy Code of Practice is a legal instrument which allows a public sector agency or organisation to make changes to an Information Protection Principle (IPP) with a Health Privacy Principle (HPP) or to specify how that rule will apply in a particular situation. Codes must not be stricter than the principles are not allowed to operate as a tool for blanket exemptions to the principles.

Both agencies and the Privacy Commissioner can prepare Privacy Codes of Practice. Agencies must consult the Privacy Commissioner when preparing Privacy Codes of Practice to modify the application of one or more IPPs or HPPs. Draft Codes need to be submitted to the Attorney General (in the case of IPPs) or Minister for Health (in the case of HPPs) who may decide to make the Code.

Important recent instruments include:

- the Privacy Code of Practice for Local Government revised 20 December 2019,
- the Privacy Code of Practice for the exchange of information by participating agencies in the Youth on Track scheme, 2018,
- the Direction relating to the "Their Futures Matter" project, 2018.

Codes must not be stricter than the principles and they should not be seen as a tool for blanket exemptions to the principles. Codes of Practice must still meet a number of requirements to ensure that they protect privacy.

Organisations not covered by the PPIP and/or HRIP Acts (e.g. state owned corporations, federal government departments, and some private sector organisations) may be covered by the Federal Privacy Act.

The Federal Privacy Act (as administered by the OAIC) also applies to all health service providers in the private sector throughout Australia: that is, to a person or entity providing a health service and holding health or personal information. The Federal Privacy Act does not apply to NSW public sector health service providers such as public hospitals which are instead covered by HRIP.

The OAIC is also the independent privacy regulator for the My Health Record system and Healthcare Identifier service and has functions and responsibilities under both the My Health Records Act 2012 and the Healthcare Identifiers Act 2010.

Other federal and NSW laws relate to data privacy, including:

- Workplace Surveillance Act 2005 (NSW)
- Surveillance Devices Act 2007 (NSW)
- Adoption Act 2000 (NSW)
- Assisted Reproductive Technology Act 2007 (NSW)
- Crimes (Forensic Procedures) Act 2000 (NSW)
- Criminal Records Act 1991 (NSW)
- Privacy Act 1988 (Cth)

- Telecommunications (Interception and Access) Act 1979 (Cth)

The NSW Privacy Commissioner does not have jurisdiction in relation to these laws and can only deal with privacy issues that arise under the PPIP and HRIP Acts.

The IPPs have been summarised by the NSW Privacy Commissioner as follows:

Collection

Lawful

Only collect health information for a lawful purpose that is directly related to the agency or organisation's activities and necessary for that purpose.

Direct

Only collect personal information directly from the person concerned, unless it is unreasonable or impractical to do so.

Open

Inform the person as to why you are collecting personal information, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, and any consequences that may apply if they decide not to provide their information to you.

Relevant

Ensure that the personal information is relevant, accurate, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

Secure

Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

Transparent

Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

Accessible

Allow people to access their personal information without unreasonable delay or expense.

Correct

Allow people to update, correct or amend their personal information where necessary.

Use

Accurate

Make sure the personal information is relevant and accurate before using it.

Limited

Only use personal information if the person has given their consent or if they were informed at the time of collection that it would be disclosed.

Disclosure

Restricted

Only disclose personal information with a person’s consent or if the person was told at the time that it would be disclosed.

Only use personal information for the purpose for which it was collected. Personal information can be used without a person’s consent in order to deal with a serious and imminent threat to any person’s health or safety.

Safeguarded

An agency cannot disclose sensitive personal information without a person’s consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person’s health or safety.

Appendix: further references

Federal

Australian Data and Digital Council

https://www.pmc.gov.au/public-data/australian-data-and-digital-council

Commonwealth

Data Sharing and Release Reforms hub

https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms

Best Practice Guide for Applying Data Sharing Principles, March 2019

https://www.pmc.gov.au/resource-centre/public-data/data-sharing-principles

Data Sharing and Release Legislative Reforms Discussion Paper, September 2019

https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf

OAIC Guide to privacy for government agencies

https://www.oaic.gov.au/privacy/privacy-for-government-agencies/

OAIC Guidelines on Data Matching in Australian Government Administration, June 2014

https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-on-data-matching-in-australian-government-administration/

OAIC Guide to data analytics and the Australian Privacy Principles, March 2018

https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/

OAIC De-identification and the Privacy Act, March 2018

https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

OAIC De-identification Decision-Making Framework

https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/

National Health (Privacy) Rules 2018

https://www.legislation.gov.au/Details/F2018L01427

Australian Government Agencies Privacy Code https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code/

https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/

National Health and Medical Research Council, Guidelines under Section 95 of the Privacy Act 1988

https://www.legislation.gov.au/Details/F2014L01500/Download

Productivity Commission, Data Availability and Use Inquiry Report, May 2017

https://www.pc.gov.au/inquiries/completed/data-access/report

New South Wales

Data Sharing (Government Sector) Act 2015 No 60

https://www.legislation.nsw.gov.au/#/view/act/2015/60/full

Data sharing generally

https://data.nsw.gov.au/sharing-data

https://www.digital.nsw.gov.au/policy/data-information/sharing-data

Understand key data legislation

https://www.digital.nsw.gov.au/policy/data-information/understand-key-data-legislation

NSW Government Data Sharing Agreement Generator - Prototype V3
https://data.nsw.gov.au/sites/default/files/2019-06/Data%20Sharing%20Agreement%20Generator%20%28prototype%29%20-%20Accompanying%20Document.pdf.pdf

NSW Government, NSW AI Ethics Framework

https://www.digital.nsw.gov.au/transformation/policy-lab/artificial-intelligence-ai/nsw-ai-ethics-framework

NSW Privacy Commissioner, Fact Sheet: Reasonably Ascertainable Identity, January 2017

https://www.ipc.nsw.gov.au/fact-sheet-reasonably-ascertainable-identity

NSW Privacy Commissioner, Direction for Domestic Violence Disclosure Scheme pilot

https://www.ipc.nsw.gov.au/sites/default/files/file_manager/PID%20-%20Section%2041%20PPIP%20-%20Domestic%20violence%20disclosure%20scheme%20pilot.pdf

NSW Privacy Commissioner, Direction under s. 41(1) of the Privacy and Personal Information Protection Act 1998 in relation to "Their Futures Matter" Project

https://www.ipc.nsw.gov.au/sites/default/files/file_manager/PID%20under%20PPIP%20Act%20-%20Their%20Futures%20Matter.pdf

NSW Privacy Commissioner, Guide – Seeking a Public Interest Direction under NSW privacy laws, October 2019

https://www.ipc.nsw.gov.au/sites/default/files/2020-01/Guide_Seeking_a_Public_Interest_Direction_under_NSW_privacy_laws_October_2019.pdf

NSW Privacy Commissioner, Privacy Governance Framework

https://www.ipc.nsw.gov.au/privacy/privacy-resources-public-sector-agencies/privacy-governance-framework

Victoria

Victorian Data Sharing Act 2017

https://www.legislation.vic.gov.au/

Victorian Data Sharing Act 2017: Guidance for departments and agencies

https://www.vic.gov.au/sites/default/files/2019-03/Victorian-Data-Sharing-Act-2017-web-guidance.pdf

Data sharing and open data portal

https://www.vic.gov.au/data-sharing-open-data

Data legislation, security and privacy

https://www.vic.gov.au/data-security-privacy

Office of the Victorian Information Commissioner, Guidelines for sharing personal information

https://ovic.vic.gov.au/resource/guidelines-for-sharing-personal-information/

https://ovic.vic.gov.au/wp-content/uploads/2018/07/Information_sharing_guidelines.pdf

Office of the Victorian Information Commissioner, De-identification and privacy: Considerations for the Victorian public sector

https://ovic.vic.gov.au/resource/de-identification-and-privacy-considerations-for-the-victorian-public-sector/

Office of the Victorian Information Commissioner, Unique Identifiers under the PDP Act https://ovic.vic.gov.au/resource/unique-identifiers/

Western Australia

Data Linkage Expert Advisory Group (Advisory Group) (led by Professor Peter Klinken AC, Chief Scientist of Western Australia), Data Linkage Review, 2016

https://www.jtsi.wa.gov.au/what-we-do/science-and-innovation/chief-scientist-of-western-australia/data-linkage-review

https://www.jtsi.wa.gov.au/docs/default-source/default-document-library/a-review-of-western-australia's-data-linkage-capabilities---developing-a-whole-of-government-model---december-2016.pdf?sfvrsn=f6c26d1c_0

Privacy and Responsible Information Sharing for the Western Australian public sector: Discussion paper

https://www.wa.gov.au/sites/default/files/2019-08/Discussion%20paper_Privacy%20and%20Responsible%20Information%20Sharing_1.pdf

Western Australian Consultation page

https://www.wa.gov.au/government/privacy-and-responsible-information-sharing

South Australia

Public Sector (Data Sharing) Act 2016

https://www.legislation.sa.gov.au/LZ/C/A/PUBLIC%20SECTOR%20(DATA%20SHARING)%20ACT%202016.aspx

Sharing public sector data

https://www.dpc.sa.gov.au/responsibilities/data-sharing/information-sharing-in-south-australia/sharing-public-sector-data

Data sharing forms and templates

https://www.dpc.sa.gov.au/responsibilities/data-sharing/data-sharing-forms-and-templates

Queensland

Access and share government data (QDAP)

https://www.forgov.qld.gov.au/access-and-share-government-data-qdap

Office of the Information Commissioner (Queensland), Privacy and sharing information between agencies

https://www.oic.qld.gov.au/publications/practice-note/privacy-and-sharing-information-between-agencies

Office of the Information Commissioner (Queensland), What is personal information? Section 12 of the Information Privacy Act 2009

https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/introduction-to-the-acts/what-is-personal-information

Algorithmic accountability frameworks for government

Directive on Automated Decision-Making, Canada

https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

US Senate, draft Algorithmic Accountability Act of 2019

https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf

New Jersey Bill A.B. 5430, draft New Jersey Algorithmic Accountability Act, introduced May 20, 2019

https://www.billtrack50.com/BillDetail/1127840

California State Assembly, draft Automated Decision Systems Accountability Act of 2020

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB2269

Robodebt

Luke Gomes, ‘Coalition warned robodebt scheme was unenforceable three years before it acted’, The Guardian, 12 February 2020

https://www.theguardian.com/australia-news/2020/feb/12/coalition-warned-robodebt-scheme-was-unenforceable-three-years-before-it-acted

Terry Carney, ‘Robo-Debt Illegality: A Failure of Rule of Law Protections?‘ on AUSPUBLAW (30 April 2018) https://auspublaw.org/2018/04/robo-debt-illegality/

Terry Carney, ‘Robo-debt illegality: The seven veils of failed guarantees of the rule of law?’, Alternative Law Journal

https://journals.sagepub.com/doi/abs/10.1177/1037969X18815913

Terry Carney, Bringing robo-debts before the law: why it’s time to right a legal wrong’, LSJ Online, https://lsj.com.au/articles/why-robo-debt-bringing-robo-debts-before-the-law-why-its-time-to-right-a-legal-wrong/#

Zalnieriute M; Moses LB; Williams G, 2019, 'The rule of law and automation of government decision-making', Modern Law Review, vol. 82, pp. 425 - 455, http://dx.doi.org/10.1111/1468-2230.12412

Cary Coglianese', Lavi M. Ben Dor, 2019, 'AI in Adjudication and Administration: A Status Report on Governmental Use of Algorithmic Tools in the United States', Uni of Pennsylvania Public Law and Legal Theory Research Paper Series Research Paper No. 19-41

Singapore

https://www.imda.gov.sg/AI

Model AI Governance Framework, 2019

Trusted Data Sharing Framework, 2019

https://www.imda.gov.sg/-/media/Imda/Files/Infocomm-Media-Landscape/SG-Digital/Tech-Pillars/Artificial-Intelligence/Trusted-Data-Sharing-Framework.pdf

UK

ICO consultation on the draft data sharing code of practice, 2019

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/

https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

ICO consultation on the draft AI auditing framework guidance for organisations, February 2020

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-ai-auditing-framework-guidance-for-organisations/

Australian Computer Society

Australian Computer Society, Privacy in Data Sharing – A Guide for Business and Government, 2017

https://www.acs.org.au/insightsandpublications/reports-publications/privacy-in-data-sharing.html

Australian Computer Society, Data Sharing Frameworks, 2018

https://www.acs.org.au/insightsandpublications/reports-publications/data-sharing-frameworks.html

Australian Computer Society, Privacy-Preserving Data Sharing Frameworks, 2019

https://www.acs.org.au/insightsandpublications/reports-publications/privacy-preserving-data-sharing-frameworks.html

Other

Desai, Felix Ritchie and Richard Welpton, Five Safes: designing data access for research, University of the West of England, 2016

http://rsss.cass.anu.edu.au/sites/default/files/rsss/Ritchie_5safes.pdf

Luk Arbuckle and Felix Ritchie, The Five Safes of Risk-Based Anonymization, IEEE Security & Privacy, 2019

Tom Burton, ‘When sharing your data is a good idea’, Australian Financial Review, 14 February 2020

https://www.afr.com/politics/federal/when-sharing-your-data-is-a-good-idea-20200214-p540p7

Tom Burton, ‘NSW pushes for stronger federal data bill to protect privacy’, Australian Financial Review, 13 February 2020, https://www.afr.com/politics/federal/nsw-pushes-for-stronger-federal-data-bill-to-protect-privacy