Privacy Update

June 2017

Overhaul of the Data Management Framework

Last month (May 2017) the Productivity Commission's Final Report into Data Availability and Use was released by the Federal Government.

In just under 100 pages, the Commission *proposed* a complete overhaul of the data management system in Australia. The report signifies a substantial evolution in the broader approach to data in Australia. Below is a brief 7-page summary of the headline challenges and opportunities that lie ahead.

Immediate Next Steps for IAB: The report proposes a complete overhaul of the Data Framework, including the creation of a new Comprehensive Right for consumers and small businesses, and new laws for the sharing and release of data.

A Cross-Portfolio Taskforce has been established by the Federal Government, headed up by Dept. Prime Minister and Cabinet (PMC) to consult with private sector over next 6mths to progress key findings in the report. IAB Australia will meet with the Taskforce to influence outcomes and create favourable policy settings for IAB members.

Below, the likely impact of the proposed overhaul of the data management framework on the core function of IAB members is outlined.

What You Need To Know

Private sector

You will need to implement processes, and policies to identify what consumer data you hold in relation to particular consumers. This is necessary from both a due diligence perspective and also to meet any new compliance requirements which might be introduced.

Responding to requests from Consumers

An outcome of the report may be the requirement to respond to requests from consumers - seeking to exercise substantial new rights - including by providing consumers with access to, and a machine-readable copy of, their consumer data.

The **New Test** for what data will be subject to this new Comprehensive Right, according to the Report, will be: *Is the data sufficient to generate a competitive offer for a consumer from another provider?*

In other words, a **New Joint Right** (discussed p3) with organisations over consumer data - might be created. Further, under proposed changes in the organisations will need to provide a readily available and easily accessible list of third parties they have shared data with over an annual, 12-month period.

The Commission identified that information asymmetry has been recognised in economics as a feature that weakens competitive markets. The proposed New Joint Right, offers a genuine two-way street to support consumers' continuing willingness to supply a crucial input to business, research and public policy — namely, their data (whether obtained directly or through other channels). Consumers would no longer be just a source of data, they would rank equally with the key data collectors — businesses and governments — in being able to trade and use their data.

NAB, ANZ, and Uber have warned the government not to define customer rights to digital data too vaguely or broadly.

"….NAB agrees in principle with proposed measures to share customers' data with other institutions and supports providing "raw data", it considers data relating to internal classifications, such as customer segmentation, pricing and fraud propensity, as commercially sensitive and proprietary".

How do you obtain consent from your consumers? You will need to consider whether more explicit consent is needed to meet the requirements of the legal reform. Alternatively, do you have a legitimate statutory basis for why you do not require express consent from a consumer? Ensure you have well documented reasons to best prepare for any changes that might be coming.

High Value Datasets

Consider whether your datasets dealt with, within your business might be designated as high value datasets (HVDs) or National Interest Datasets (NIDs), and accordingly whether those datasets might be required to be disclosed to government agencies or the broader market.

A key facet of the recommended reforms is the creation of a data sharing and release structure that indicates to all data custodians a strong and clear cultural shift towards better data use that can be dialled up for the sharing or release of higher-risk datasets.

For datasets designated as national interest, all restrictions to access and use contained in a variety of national and state legislation, and other program-specific policies, would be replaced by new arrangements under the *Data Sharing and Release Act*.

National Interest Datasets would be resourced by the Commonwealth as national assets.

A suite of Accredited Release Authorities (ARA) would be sectoral hubs of expertise and enable the ongoing maintenance of, and streamlined access to, National Interest Datasets as well as to other datasets to be linked and shared or released. A streamlining of ethics committee approval processes would provide more timely access to identifiable data for research and policy development purposes.

Particularly for larger publishers, with access to any type of health-related data, immediate legal counsel should be sought on what data sets might be considered High Value Data sets.

Disclosure

Government agencies would need to implement processes (in conjunction with stakeholders) in relation to data sharing and management, de-identification and the 'comprehensive' right.

Government agencies would be required to disclose all information that they hold which is not personal, commercial in confidence or related to national security.

Government agencies would have a greater right to access and require the release of information held by the private sector. This is a low risk for the private sector.

Consumers' new 'joint right' with organisations over their consumer data

Consumers would have a much broader right to access a greater quantity of information you store about them, and consumers will also have greater right to control how you transfer information to a third party to improve the ability to make decisions about, and to acquire, products and services.

Individuals would be provided with greater access to searchable, comprehensive public datasets.

Under the proposed Comprehensive Right, the Commission suggests a genuine two-way street where a consumer must expressly state their support and continuing willingness to supply a crucial input to business, research and public policy — namely, their data (whether obtained directly or through other channels).

Ride sharing app Uber is concerned that mandatory data sharing "could undermine the commercial incentives that drive business innovation". Uber said this would be "particularly true if there is a real or perceived risk that competitors may gain access to that information" and called for assurances "that commercially sensitive information required to deliver such innovations is not undermined".

Consumers would no longer be just a source of data, they would rank equally with the key data collectors — businesses and governments — in being able to trade and use their data.

Consumers in effect will have a 'joint right' with organisations over their consumer data. In addition, organisations would also be required to disclose the third parties with which an organisation trades, or otherwise discloses, consumer data. Organisations will not be required to advise consumers on all occasions data is shared, but they will need to provide an easily accessible list of parties they have shared data with over an annual period.

Data Sharing and Release Act (DSRA) – new laws and legislation

A structure for data sharing and release will be introduced, under proposed reforms, that would allow access arrangements to be 'dialled' up or down according to the nature of risks associated with different types of data, uses and use environments.

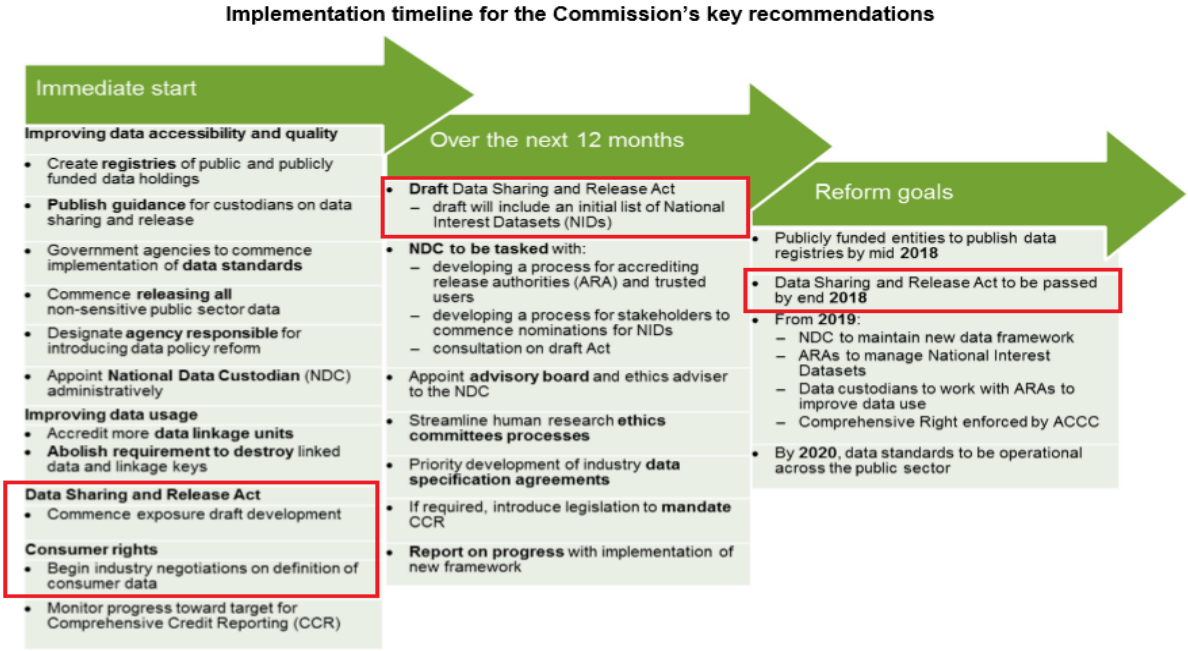
Implementation and ongoing monitoring of the laws would be vested with a new statutory office holder, the National Data Custodian (NDC).

The NDC would administer the *DSRA* and recommend valuable datasets for designation as National Interest Datasets, provide technical guidance and direction to the data system, accredit and coordinate Accredited Release Authorities (ARAs), report on data use 'good news' and breaches, and manage broader ethical considerations within the data release and sharing system.

An integral part of the Commission's recommended data reform Framework is the introduction of a network of the ARAs.

ARAs would be hubs of sectoral expertise in data curation, de-identification and linkage, would implement a risk-based approach to the broader sharing and release of data through formal, contemporary, NDC-reviewed risk management procedures.

Implementation Plan



Immediate Next Steps for IAB:
IAB Australia will contribute to industry consultation undertaken by the government involved in the creation of proposed new Commonwealth legislation — the DSRA.

By giving consumers new rights to use their digital data and data holders permission to be pro-active about data possibilities, the DSRA creates a new lens through which to view data; the lens of a valuable asset being created, not merely a risk or an overhead.

IAB Australia will advocate striking the right balance in upholding consumer rights to privacy without watering down proprietary rights of business, and maintaining an innovative and competitive environment for digital operators reliant on data.

Consumer Data – shifting definitions

The Commission has recommended, at its broadest level, consumer data should include:

- personal information (defined in the *Privacy Act 1988 (Cth)*) that is in digital form
- files posted online by the consumer
- data created from consumers' online transactions, Internet-connected activity or digital devices
- data purchased or obtained from a third party that is about the identified consumer
- other data associated with transactions or activity that is held in digital form and relevant to the transfer of data to a nominated third party.

Immediate Next Steps for IAB:

Current data practices now support inferred information about personal behaviour and preferences. This does not directly or indirectly identify a person and is a category of digital data which has ambiguous status within the privacy regulatory framework.

The definition of "consumer data" is now up for debate as part of the reform. Industry consultation is being sought on the correct definition. IAB Australia will seek to positively influence government consultation around what is the best definition of consumer data to create an operating environment for IAB members.

Background – Privacy Law in Australia

In 2014 new changes were introduced including the following: a new system of privacy principles; enforcement mechanisms; and the introduction of a civil penalty regime for breaches of privacy. To comply with the laws, privacy policies were updated and practices, procedures and systems were revised and implemented.

The changes introduced in 2014, are still relevant today, and form the foundation upon which the current overhaul of the Data Management Framework (discussed above) is occurring.

13 new 'Australian Privacy Principles'

The National Privacy Principles (NPPs) applicable to the private sector, and the Information Privacy Principles (IPPs) applicable to the federal public sector, were replaced with a united set of 13 new 'Australian Privacy Principles' (APP) to regulate the handling of personal information.

The big change in Australia in 2014: the bar was dramatically raised in terms of what was expected from companies.

It was no longer sufficient for any private sector organisation to simply have a privacy policy regarding personal information. There was a new obligation to **take reasonable steps** ***to implement practices, procedures and systems that comply with the Australian Privacy Principles.***

The APPs imposed obligations on both Commonwealth agencies and private sector organisations at every stage in the cycle of handling personal information. Many existing principles were expanded and new obligations were introduced. In both cases, the changes created more prescriptive requirements for the handling of data.

Businesses were required to introduce a **privacy policy** that covers specific types of information under the 2014 changes to privacy and implement practices, procedures, and systems that cover the handling of specific types of information.

In the digital age, information can be transmitted easily and quickly. The changes required companies to de-identify or destroy **unsolicited personal information** as soon as practicable if that information is not necessary for one or more of the private sector's core function.

Health information and a new general rule was implemented for the collection of sensitive information which requires an entity to obtain the individual's prior consent.

Direct marketing a new ban on the use and disclosure of personal information by organisations for direct marketing purposes. In addition to the current framework of specified circumstances and exceptions, a consumer who receives unsolicited direct marketing gains an important new right to force a company to disclose the source of the individual's personal information.

Power and Penalties

Under the key reforms made to the *Privacy Act 1988 (Cth)* by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth),* the national privacy regulatory, the Office of the Australian Information Commissioner (OAIC) had functions and powers expanded included the following functions:

- ***Investigations*** – power to investigate and monitor compliance with privacy obligations and conduct privacy performance assessments.

- ***Enforceable undertakings*** – the power to accept enforceable undertakings by companies to take, or refrain from taking, action that may be enforced in court

- ***Civil penalty orders*** – the regulators can now apply to the Federal Court or Federal Circuit Court for a civil penalty order.