SUMMARY REPORT

DATA TO DECISIONS CRC
UNLOCKING THE VALUE OF AUSTRALIA'S DATA

# INFORMATION SHARING

**Information sharing between agencies is a complex yet vitally important area. The need to improve information and intelligence sharing in the national security community has been mentioned in numerous reports and strategies over many years, at least fifteen since 2007.**

**However, delivering actual improvements is challenging due to a complex and outdated legal landscape, a real need for secrecy in some circumstances, and legitimate concerns about data privacy and security.**

One problem facing information sharing in the national security community is the complexity of and the lack of a coherent principle underlying distinctions that are drawn around which agencies can access which data for what purposes. Related to this complexity – it is very hard to have a public, or even political, debate around data sharing laws given the generally low level of understanding of what is permitted and in which circumstances.

Another problem is that the laws are drafted around assumptions about how data is stored – there are still assumptions that a single entity owns or controls particular data. Integrity of data and the strength of inferences drawn from it can also create complexities. People often worry about data being used inappropriately to make adverse decisions with negative consequences for individuals, particularly where information is taken out of context. Something may be inappropriate in one context (like a joke about bombs at an airport) but appropriate in another, and words may have different meanings in different agencies and databases.

There needs to be clarity and transparency around how, generally speaking, data about people is collected, accessed and used by government in a variety of contexts. Over the longer term, this requires a major overhaul of existing laws so that they can be reframed in a principles-based, risk-based framework that those affected can understand and debate. Information flows within the national security community can be made more efficient, but only within a framework that maximises transparency (within the limits of justified operational secrecy) thus ensuring a public licence to operate. It is also necessary to ensure that responsibilities for data, in particular its security, confidentiality, preservation, destruction, and disclosure, are clearly and appropriately allocated. The recommendations also take into account the challenges faced within agencies in facilitating appropriate information flows.

The Data to Decisions CRC, Law and Policy Program launched this project, together with a project on data governance, to better understand how appropriate information sharing for national security purposes could be enabled while maintaining or enhancing important protections and necessary secrecy. The research was commissioned by the Australian Criminal Intelligence Commission and was conducted independently by researchers from UNSW Law, supported by researchers at La Trobe University. All of the recommendations are made by the research team based on doctrinal and empirical research conducted. While they take into account research participants' ideas, they are not necessarily advocated by any particular research participant.

> “
>
> It is also necessary to ensure that responsibilities for data, in particular its security, confidentiality, preservation, destruction, and disclosure, are clearly and appropriately allocated.

*National security refers to intelligence, law enforcement and defence.

Summary of Recommendations

# RECOMMENDATIONS FOR THE MEDIUM TERM

1

## MEANING OF DISCLOSURE

Interpretation legislation should be amended to provide for a clear and consistent definition of "disclosure" that distinguishes between disclosure of information and discoverability of information (incorporating metadata about that information) as well as between making information accessible and actually copying or transferring information.

2

## MEMORANDUM OF UNDERSTANDING

Clear allocations of powers and responsibilities for information should be made subject to a system-level memorandum of understanding or a series of standardised memoranda of understanding (or similar document/s) that sets out the agreed information governance framework.

3

## EMPOWER LEADERSHIP

Agencies should secure the support of senior leaders in partner agencies and encourage them to build accountability and incentive structures that recognise the contribution made through accurate and timely recording and sharing of information and intelligence. This process should be assisted through measurement, auditing and reporting on information made available and used/accessed through the platform.

4

## TRAINING

Training should be used as an opportunity to bring officers from different agencies together, clarify rules and expectations around information sharing (with clear written guidance), encourage and explain common ontologies/terminology, and explain responsibilities including citation and acknowledgement of original and intermediate information and intelligence sources.

5

## DATA MATCHING

Data providers should seek an exemption from the Office of the Australian Information Commissioner in relation to the Guidelines on Data Matching in Australian Government Administration, and from relevant privacy officers in other jurisdictions with similar guidelines. This will provide some assurance to agencies that are bound by privacy laws that the use of data under their control for data matching is not in breach of their obligations.

Summary of Recommendations

# RECOMMENDATIONS FOR THE LONG TERM

6

## SINGLE APPROACH

The legal framework for information sharing should be simplified by bringing disparate laws together in one place rather than amending different pieces of legislation. This would be a single Commonwealth Act containing rules for how and when Commonwealth data is collected, distributed, accessed, used, stored and deleted. While this could preserve some distinctions for specific data sets or agencies (based on differential risk), it would provide a common framework for Commonwealth data. Potentially, this could become a model for similar laws in each State and Territory. There should be opportunities for public engagement in formulating the new law.

7

## TERMINOLOGY

As part of this new Act, legislative terminology around access to, use of and disclosure of data within and among Commonwealth, State and Territory entities should be clarified.

8

## POSSESSION

The idea of "data ownership" or "possession of data" is confusing and unhelpful. In the new Act, legislative drafters should avoid property language in linking information and electronic documents to agencies. Over time, it should also be removed from existing statutes. Legislation, including archiving, privacy, freedom of information, subpoena and agency-specific rules, should use consistent, precise language to specify which agency has responsibility for which data. Responsibility should be allocated based on the variety of functions that may be performed by an agency in relation to specific data including entitlement to access, stewardship/control, possession of physical media on which information is stored, and different categories of service providers (including platform/architecture and data analytics).

9

## RESTRICTIONS ON DISCLOSURE

Legislation often seeks to reduce risks of privacy harms and inappropriate use of information through rules that restrict the disclosure of information, including within government. While risk should be assessed and managed or avoided, it is not clear that information governance should rely so heavily on retention of control of information within a particular agency, particularly where disclosure occurs between Commonwealth agencies, but also where it occurs between Commonwealth and State or Territory agencies. Conditions associated with "use" of information should be used in some circumstances where it is important that information be treated as a "national asset" in a changing technological environment.

Summary of Recommendations

# RECOMMENDATIONS FOR THE LONG TERM

10

## PRINCIPLES-BASED APPROACH

A consistent approach should be pursued across the Commonwealth, States, Territories and private sector to ensure seamless information sharing. While restrictions on data discoverability, disclosure (particularly to a different level of government or the private sector), use and action will often be appropriate, these need to be justifiable, clearly articulated and technology neutral.  Such a shift needs to be accompanied by an appropriate information governance framework (D2D CRC has developed such a governance framework in another project).

11

## RISK-BASED APPROACH

Principles-based restrictions on discoverability of, access to, use of or action based on data should recognise and support a risk-based approach to specific data elements based on data sensitivity, security risk and alignment of purpose. This risk-based approach should be enabled by legislation and detailed in regulations, standards, memoranda of understanding/letters of agreement, guidelines and/or standard operating procedures. To the extent that disclosure does not create operational risk, these rules should be publicly available to support the public licence to operate.

For information about the full report please contact **info@d2dcrc.com.au**

RECOMMENDATIONS IN BRIEF

MEANING OF DISCLOSURE

MEMORANDUM OF UNDERSTANDING

EMPOWER LEADERSHIP

TRAINING

DATA MATCHING

SINGLE APPROACH

TERMINOLOGY

POSSESSION

RESTRICTIONS ON DISCLOSURE

PRINCIPLES-BASED APPROACH

RISK-BASED APPROACH