SUMMARY REPORT

HIGH LEVEL PRINCIPLES

The Law and Policy program of the Data to Decisions CRC (D2D CRC) identified a set of high level principles to guide the development of recommendations concerning a regulatory framework for the appropriate use of Big Data for defence, national security and law enforcement (DNSLE) purposes.

Authors:
Professor Lyria Bennett Moses, Project Leader, UNSW Law
Professor Louis de Koker, Program Lead, La Trobe University
Dr Sarah Logan, Lecturer, Australian National University

The set reflects insights gained in the course of a five-year program of research in a number of research projects on specific aspects of the use of Big Data in national security and law enforcement. This document is a summary version of a more extensive report available on the D2D CRC website.

High level principles are not themselves a legal or regulatory framework but have been created for the purposes of:

- assessing existing and proposed legal frameworks, reflective of emerging "best practice" in relation to matters such as privacy and data protection, record-keeping, data governance, and protective security; and
- assessing existing and proposed socio-technical systems used for data processing (systems), including design specifications and procurement standards, in line with a compliance through design approach in relation to privacy and data protection, record-keeping, data governance, and protective security.

The principles were authored by researchers in the final research project of the Law and Policy Program of the D2D CRC and reflect the view of those authors, after consultation with government agencies, civil society organisations and within academia. They have not been adopted, directly or by implication, by the Australian government or by any of the DNSLE agencies participating in the D2D CRC or other individuals or groups consulted. These principles have been developed with the Australian context in mind.

High level principles exist in a culture of interpretation. They might be interpreted as broad and constraining or as a compliance requirement to be overcome. Should these prinicples be adopted, it is important that they are interpreted in light of rule of law values and with a mindset geared towards stewardship as opposed to minimalist or technical compliance.

TERMINOLOGY

Information lifecycle, in this document, includes collection, access, merger, matching, linking, aggregation, correction, data discovery, disclosure, sharing, publication, analysis, retention, storage and erasure.

Personal information defined in Privacy Act 1988 s 6(1)

Processing of data or information includes creation, access, collection, storage, scrubbing, linking, merging, altering, sharing, aggregating, searching, discovering or otherwise using data/information (see "information lifecycle" above, but noting erasure is not "processing" in our definition).

Proportionality is a comparative relation of one thing to another as respects magnitude, quantity or degree. In relation to fundamental rights, the Australian High Court employs proportionality analysis to ascertain the rationality and reasonableness of the restriction on the fundamental right: the greater the restriction on the fundamental right, the more important must be the public interest purpose of the legislation for the proposed restrictive measure to be proportionate.

Appropriate in this document means reasonable and justifiable in an open and democratic society in light of anticipated benefits, costs and risks for affected parties.

Regulatory Framework in this document, is a framework comprising a sustained and focussed attempt intended to produce a broadly defined outcome or outcomes directed at a sphere of social activity according to defined standards or purposes that affect others in order to address a collective concern or problem, and can include laws, formal regulations, policies, procedures and elements of technological design.

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

RISKS AND OPPORTUNITIES

The use of Big Data for DNSLE purposes offers new opportunities. It may improve the efficiency of national security and law enforcement analysis, possibly leading to faster and better insights, including by identifying and assessing potential threats.

It also creates risks, particularly for data subjects, for example relating to over-collection of data, the use of inaccurate or incompatible data, the use of inappropriate, biased or inaccurate analysis, the generation of unjustified or untested inferences, biased or inaccurate analysis, the generation and (as a result) the making of unfair or unjustified decisions, potentially involving differential treatment of people with particular innate characteristics.

Current rules are not necessarily designed to maximise these opportunities and detect, investigate, avoid, prevent and/or mitigate the risks effectively. A regulatory framework that reflects these high level principles collectively and comprehensively will, in the view of the Law and Policy program, enable the use of appropriate technologies while providing important protections and oversight.

SUMMARY OF HIGH LEVEL PRINCIPLES

A

JUSTIFICATION AS REASONABLY NECESSARY

DSNLE agencies should only process personal information in circumstances justified as reasonably necessary to achieve defined and legitimate DNSLE objectives.

PROPORTIONALITY

B

The design, operation and management of all elements of the information lifecycle, including the processing of Big Data for DNSLE purposes, must be proportionate.

Measurement of the likelihood and severity of any risk to data subjects needs to done with an understanding of context, including the category of data subject (offender, suspect, victim, witness, etc), nature of the data and the manner of processing.

C

CLARITY, CONSISTENCY AND PREDICTABILITY

The regulatory framework should be clear and consistent and the application of its rules should be predictable in foreseeable circumstances.

The regulatory framework should be easy to navigate. It should be terminologically consistent, logically consistent and normatively consistent. Rules should be broad and agile while being specific enough to avoid ambiguity, and so maintain auditability.

D

INTEGRITY AND RELIABILITY

Integrity and reliability of data and analysis should be supported by law, regulation and systems design.

Where integrity of data or techniques is assessed as low, so that inferences drawn therefrom would be unreliable, decisions about retention or use should reflect that fact.

E

SECURITY

Data and systems must be protected from illegitimate access and use.

Technical, management and governance measures must include procedures empowering individuals to report concerns or breaches internally and require appropriate reporting to oversight agencies and regulators, and, where appropriate (and after internal and oversight mechanisms are utilised), alerting individuals and organisations affected by an adverse event.

F

ACCOUNTABILITY AND EXPLAINABILITY

Laws, regulations and systems should ensure the accountability of DNSLE agencies and officers.

Internal and external accountability is required for systems design and procurement, the processing of data and the making of decisions based on inferences drawn from data processing. Auditing, oversight and accountability mechanisms and their enforcement need to be appropriately resourced (including in terms of technical expertise) and backed by appropriate sanctions.

G

REVIEW

Laws, regulations, processes and systems should be reviewed initially, regularly and when warranted.

Principles, rules, processes and systems should be subject to regular, transparent review, and be reviewed, when warranted, internally and by independent external bodies. Reviews, evidence and evaluations should feed back into the strategy and methods of DNSLE agencies, the design of the regulatory framework and specific future application of all other Principles.

H

TRANSPARENCY

The regulatory framework should support openness and transparency while safeguarding operational secrecy, where reasonably necessary.

Agency powers regarding the collection of, access to and use of Big Data, justifications for those powers, and the regulatory framework itself should be clear to interested members of the public and those potentially adversely affected by decisions. Operational secrecy should be limited to circumstances in which it is reasonably necessary. This Principle has implications for procurement.