Project D: Articulating law and policy principles for guiding Big Data usage for defence, national security and law enforcement purposes

Policy Report:
High Level Principles

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

With thanks to:

The broader Data to Decisions CRC Law and Policy team (2014-2019).

Stakeholders who contributed and provided feedback on earlier drafts of this document, both in workshops and through correspondence.

11 June 2019

I. Introduction

This report identifies 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. The report, compiled by the Law and Policy Program of the Data to Decisions Cooperative Research Centre (D2D CRC), 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.

1. Objective of this report

The objective of this report is to articulate the Law and Policy Program's understanding of the key governing principles as it evolved in accordance with new literature and our own research findings throughout the D2D CRC. These are principles against which we believe:

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

The report is being prepared near the conclusion of the Data to Decisions CRC in order to share what has been learnt by researchers in the D2D CRC Law and Policy Program, in particular through projects and activities conducted with stakeholders in DNSLE and policy agencies. There are several factors that, in combination, suggest the importance of this exercise:

- New data science techniques create an opportunity to gain insights from Big Data. These methods create new opportunities but also generate new risks and harms, particularly in relation to privacy, fair and equal treatment of individuals, and abuse of power.
- The D2D CRC has developed new Big Data tools for DNSLE agencies; the role of the Law and Policy program includes assessing legal, ethical and policy issues associated with the development and use of such tools. The role of the Law and Policy program included initiating and facilitating conversations about these issues with D2D CRC management and technical researchers.
- The Law and Policy program worked directly with DNSLE and policy agencies on a range of projects relating to the use of Big Data for DNSLE purposes. These included projects around identity assurance, information sharing, data governance, the use of "open source" data, and compliance through design. The role of the Law and Policy Program in these projects included analysis of existing regulatory frameworks and developing proposals for reform.
- Specific decisions about what laws and control measures ought to apply, both in the specific context of the use of Big Data for DNSLE purposes, and more broadly, are often controversial. However, there is potential for greater consensus at the high level at which these principles are drafted.
- It is desirable that conversations around the appropriateness of existing regulatory frameworks and the development of reform proposals be based on a common understanding of the principles on the basis of which such arguments are made. Especially where reasonable minds may differ on the appropriate high level principles to be applied, it is important to be explicit about which principles have been deployed.

The principles are authored by researchers in the final research project of the Law and Policy Program of the Data to Decisions CRC. 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. While these principles are informed by earlier drafts produced by the Law and Policy program, the current version reflects the opinions of the authors of this document and not necessarily all researchers who have worked on D2D CRC projects over the period 2014-2019.

These principles are not intended to duplicate or replace aspects of existing regulatory frameworks or technical standards, nor are they intended as articulating a new regulatory framework. For example, they do not interact directly with legislation such as the *Privacy Act 1988* (Cth) and do not provide a similar level of detail. They operate at a "high level", providing a normative framework against which regulatory frameworks and technical standards can be evaluated in the context of the use of Big Data for DNSLE purposes. But they do not attempt to prescribe things that agencies can or cannot do: rules governing agency practices are found in legislation, regulations, inter-agency agreements, mandated standards, and elsewhere. This report is not itself a regulatory instrument, and there is no proposal that it become one.

These principles have been developed with the Australian context in mind, but with an eye to learning from similar exercises in comparable jurisdictions studied throughout the Law and Policy Program.[1]

The primary audience thus comprises:

- policy agencies (responsible for legislation regulating data processing by DSNLE agencies),
- those responsible for systems design specifications and procurement (adopting a compliance through design approach, these systems are themselves regulatory), and
- civil society (as a basis for support or critique of the existing regulatory framework by reference to agreed principles)

Data analysts in DSNLE agencies are *not* the primary audience for this document. These analysts are expected to comply with existing law and use systems as designed. Because the principles are directed at the regulatory framework and not at specific actors (such as data analysts working in DNSLE agencies), they are not properly described as ethical guidelines. There are ethical guidelines that have been proposed in related contexts,[2] but the purpose of these high level principles is distinct.

The principles are not intended as comprehensive. The reach of the High Principles below is limited by the research projects on which the Law and Policy program has been engaged and the topics we have had the opportunity to explore. Further, there is much more that can be said about principles such as transparency and proportionality. This document is however intended to provide a normative framework for evaluation; more detailed analysis can be found in the reports and publications of the Law and Policy Program of the D2D CRC (and elsewhere in the academic literature).

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 principles 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.

This document remained live throughout the duration of the D2D CRC, with amendments made and communicated as insight deepened or consensus developed. It was presented in final form at the end of the D2D CRC, along with specific recommendations arising from D2D CRC Law and Policy projects.

Throughout the D2D CRC and specifically towards its end, we engaged with government agencies (including the Attorney General's Department), civil society organisations and within academia. Although such engagement enhanced the insights underpinning the report, not all suggestions have

[1] For example, see *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, RUSI, 2015

[2] Eg Data61, *Artificial Intelligence: Australia's Ethics Framework: A Discussion Paper* (2019), Accenture, *Universal principles of data ethics*; Data Science Organisation, *Code of Conduct*

been adopted and thus mere engagement with the drafters (specifically by government agencies and civil society organisations) does not amount to their endorsement of the principles.

2. Terminology

Big Data is a controversial term, but is intended here to refer to large, diverse or evolving[3] data collections that may be processed (data processing defined below). While we acknowledge the importance of questions relating to the sharing of specific information about an individual or a small number of individuals between agencies in response to a specific request, and we are mindful that complex data analysis can also be carried out with smaller data sets, this report focuses on larger or "bulk" data sets. This decision is not justified normatively (and terminology in this area continues to shift), but to ensure alignment with the scope of D2D CRC research projects conducted by the Law and Policy program.

The **information lifecycle**,[4] for purposes of this report, includes:

(a) Collection of data for DNSLE purposes,
(b) Access to data by DNSLE agencies (including government data, privately held data (held in Australia or overseas), data held by foreign governments accessible through partnerships, and publicly available data), including decryption of encrypted data where appropriate,
(c) Data merger, matching or linking,
(d) Data aggregation
(e) Correcting data (including data scrubbing),
(f) Facilitation of data discovery (for example, by allowing DNSLE agencies to search over data held centrally or in another agency),
(g) Disclosure or "sharing" of data (within government, within Australia and with foreign governments/agencies), including open publication of data (where permitted, including through treaties and partnerships),
(h) Data analysis,
(i) Data retention and storage (within government or mandated by government in accordance with relevant records retention and management policies), and
(j) Data erasure.

Personal information is 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). Data can also be derived from other data, or in other words "created" from data, as well as from sensors and individuals. The processing of data will often include specific techniques such as machine learning, although the focus here is on data practices rather than on what is sometimes described as artificial intelligence " (although there is obviously overlap).

Proportionality[5] is a comparative relation of one thing to another as respects magnitude, quantity or degree. In relation to fundamental rights, the Australian High Court,[6] employs proportionality analysis to

[3] Referring to the three V's – volume, variety, velocity. See Pompeu Casanovas, Louis de Koker, Danuta Mendelson and David Watts, 'Regulation of Big Data: Perspectives on Strategy, Policy, Law, and Privacy' (2017) 7 *Health and Technology* 335, 336.
[4] The definition here is broad in order to clarify the scope of the Policy Paper. By listing activities here, we are not implying endorsement, either generally or in specific cases. We are not considering some activities, in particular de-identification and re-identification, within this Policy Paper.
[5] This approach to proportionality is informed by the High Court's decisions in *Unions NSW v New South Wales* [2013] HCA 58; at [55]-[56]; *Murphy v Electoral Commissioner* [2016] HCA 36 at [64]-[65], *McCloy v New South Wales* [2015] HCA 34 at [87] and [67]. The discussion of proportionality was contributed by Professor Danuta Mendelson.
[6] "The term 'proportionality' in Australian law describes a class of criteria which have been developed by this Court [the High Court of Australia] over many years to determine whether legislative or administrative acts are within the constitutional or legislative grant of power under which they purport to be done." *McCloy v New South Wales* [2015] HCA 34 at [3] per French CJ, Kiefel, Bell and Keane JJ.

"ascertain the rationality and reasonableness" [7] 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.

Adapted to the context of these principles, proportionality analysis comprises of the following components/questions:

1. Whether the legislation or a particular measure/action by the DNSLE agency that will result in limiting a fundamental right pursues a legitimate specific objective (one that does not impinge upon the functionality of the system of representative government) of sufficient importance to warrant limiting this right;
2. If so, whether the proposed means (including processing of data) in service of the objective are rationally connected (suitable) to the specific objective;
3. Whether the rights-limiting means in service of the objective are necessary to achieve that objective. In other words, are there alternative reasonably practicable means of achieving the same purpose without impairing, or significantly impairing the fundamental right. For example, an alternative reasonably practical means may include restricting the access to or adopting a more narrowly focussed collection of data. If, and only if, these alternative measures are identical in their effects to the measures which have been chosen, the proposed measure is not necessary.
4. Whether the proposed measure involves adequate balance between the importance of the law's proper purpose to be furthered by the restrictive measure and the extent of the restriction it thereby imposes on the fundamental right. The balancing process for ascertaining proportionality requires examination and evaluation of evidence but does not include determining policy or fiscal choices.

This report adopts "proportionality" as a guiding principle for understanding the extent to which Big Data should be used for DNSLE purposes. Data practices have the potential to infringe fundamental rights inherent in the rule of law and international human rights, including the right to privacy, the right to equal treatment under the law, and the right to protection from abuse of power. Any impact on these fundamental rights should be proportionate to public interest purposes associated with the use of Big Data for DNSLE purposes.

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, for the purposes of this report, 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,[8] and can include laws, formal regulations, policies, procedures and elements of technological design.

[7] *Murphy v Electoral Commissioner* [2016] HCA 36 at [65] per Kiefel J.

[8] Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2 *Regulation and Governance* 137, 139; Karen Yeung, 'Are Human Biomedical Interventions Legitimate Regulatory Policy Instruments?' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook on the Law and Regulation of Technology* (2017) 823, 834-5.

II. High level principles on the use of Big Data for DNSLE purposes

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, and (as a result) the making of unfair or unjustified decisions, potentially involving differential treatment of people with particular innate characteristics.[9] 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.

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.

This objective can be achieved by limiting agency powers in line with agency functions as well as procedures and processes that require explicit justifications for data processing. Personal information should not be retained for longer than can be justified as reasonably necessary.

B. Proportionality

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

Practices (in particular the use of Big Data for DNSLE purposes) and controls (through law, regulation, design and processes) must be proportionate within the meaning set out above and in line with the justification referred to in Principle A. 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 (to the extent possible across jurisdictions), logically consistent (for example, not simultaneously prohibiting and requiring a particular activity) and normatively consistent (for example, not making arbitrary distinctions that lack normative justification). Rules should be broad and agile enough to operate in a dynamic environment while being specific enough to avoid ambiguity, and so maintain auditability. Secret interpretations that deviate from plain language understandings or ordinary interpretations of a statutory provision would not be considered predictable for the purposes of this Principle.

[9] Opportunities and risks are outlined in reports of the D2D CRC project entitled 'Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law'.

D. Integrity and reliability

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

The regulatory framework and design specifications should, so far as is possible, support:

- the integrity of data collected, retained and accessed by government for DNSLE purposes, and
- the reliability of analytical and decision-making uses of such data and systems in light of data integrity and context of use (including the potential for harm or disparate impact).

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.

The security of relevant data and systems, both within and outside DNSLE agencies, must be kept safe from internal and external security breaches in line with the sensitivity of data held and existing legal requirements and technical standards. In particular, access should be limited to appropriately authorised and trained personnel. 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.

Systems should be designed so that access to data and analysis of data is tracked, recorded and audited for justification, security and intrusiveness, both internally and through relevant forms of oversight (executive, independent, Ministerial). Compliance by Design principles should be implemented to ensure that systems operate in compliance with legal requirements. Where appropriate, Compliance through Design[10] approaches should support human decision-takers. Decisions made on the basis of inferences drawn from data processing should be subject to appropriate internal governance and auditing as well as effective, independent and Ministerial oversight and accountability. Similarly, decisions on design specifications for systems deployed need to be justified with reference to purpose, capabilities, limitations and risks, and always be subject to oversight. Auditing, oversight and accountability mechanisms and their enforcement need to be appropriately resourced (including in terms of technical expertise) and backed by appropriate sanctions.

Human decision-makers should remain accountable for decisions of DNSLE agencies that produce significant adverse legal or practical effects for individuals. Where decisions are based on inferences drawn from data processing, accountability requires that decision-makers (including, where relevant, oversight bodies and judges) have a sufficient understanding of the provenance, meaning and quality of data, of any sources of incompatibility among the meanings and qualities of the different sources of data, of the applicability of the analytical procedures to the relevant kinds of data, and of any biases or other weaknesses in the analytic process. This requirement of explainability may be achieved through a variety of means, including choice of process (for example, explainable artificial intelligence) or evaluation and testing (including for particular biases) of inputs and outputs of otherwise opaque processes.

Accountability is essential to protect individuals adversely affected by DNSLE decisions based on inferences drawn from data processing. Executive, independent and Ministerial accountability are also necessary to promote trustworthiness and, hence, public confidence in DNSLE agencies.

[10] Pompeu Casanovas, Jorge González-Conejero and Louis de Koker, 'Legal Compliance by Design (LCbD) and Through Design (LCtD): Preliminary Survey' in Víctor Rodríguez-Doncel, Pompeu Casanovas and Jorge González-Conejero (eds), *Technologies for Regulatory Compliance* (CEUR Workshop Proceedings vol 2049, 2018) 33.

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. The reviews need to consider the alignment with DNSLE objectives (see Principle A), alignment with other principles, the impact of new developments in technology, potential for abuse. They should provide evidence (including through evaluation) as to whether the system delivers intended results effectively, efficiently, reliably and is proportionate to impacts on civil liberties, legal rights, and other individual and collective interests. The nature of such review is contextual but should include a privacy impact assessment and community engagement where relevant. Reviews will be warranted when there is a specific risk or evidence of abuse, and should result in improved mitigation of such risks in the future. 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 governing the use of those powers should be clear (a) to those with an interest in policy- and rule-making (including the public) to facilitate public debate and democratic accountability, and (b) to those potentially adversely affected by decisions. Operational secrecy should be limited to circumstances in which it is reasonably necessary, and decisions to keep information secret should be accountable (see Principle F).[11] Procurement should have regard to (1) the extent to which software can form part of an accountable decision-making system (Principle F), and (2) any contractual terms or intellectual property rights that restrict transparency (beyond the need for operational secrecy).

Transparency is an enabling Principle, facilitating evaluation of practices and regulatory frameworks against other Principles.

[11] Lyria Bennett Moses and Louis de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41(2) *Melbourne University Law Review* 530, 542-4.