3/2/18

To whom it may concern,

Please find below a submission to the enquiry into the Impact of New and Emerging Information and Communications Technology (ICT) by the Parliamentary Joint Committee on Law Enforcement. This submission is made by the Law and Policy Program of the Data to Decisions Cooperative Research Centre (D2D CRC). We appreciate the committee's time and consideration on this important topic and are happy to participate further at the committee's request.

Please contact me as the representative of the Data to Decisions Cooperative Research Centre's Law and Policy Program if you require any further information.

Sincerely,

Dr Sarah Logan

Postdoctoral Research Fellow
Law and Policy Program
Data to Decisions CRC
UNSW Law

Introduction

The Data to Decisions Cooperative Research Centre (D2D CRC) is part of the Cooperative Research Centres Programme and was established in July 2014 with a grant of $25 million from the Australian government. The D2D CRC brings together researchers and industry to address the Big Data challenges that face Australia's national security agencies. The D2D CRC works collaboratively with a range of government industry and academic participants.

The Law and Policy Program is one of four research programs maintained by the CRC. The Program investigates aspects of the policy and legal framework required to support appropriate implementation of the tools developed by the CRC, especially to balance societal and individual interests. The Law and Policy Program is led by Professor Louis de Koker (La Trobe Law School) and shared between La Trobe Law School, UNSW Law and Deakin Law School. Research projects undertaken in the Program are informed by the needs of government end-users, channelled through the Attorney-General's Department as the government lead on appropriate laws and policies in the national security and law enforcement space.

Summary

This submission outlines the Law and Policy Program's research on issues of relevance to the committee and makes seven recommendations drawing on this research.[1] These recommendations relate to the committee's ToR A (1 - 7) and ToR B (6, 7). Overall, our research has found that changing technology has rendered some of the existing law and policy regarding use of such technology by law enforcement agencies outdated or confusing, creating challenges for information sharing and use of open source data by law enforcement agencies. The complexities of enhanced data analytics similarly create governance challenges, requiring appropriate attention to governance capacity and capabilities.

Background

These recommendations draw on the findings of two research projects recently completed by the Law and Policy program and one currently underway.

a) The first project, completed in August 2017, is titled *Information sharing and the National Criminal Intelligence System (NCIS)*. The project examined barriers to information sharing among state and federal law enforcement agencies as a subset of barriers to the implementation of the NCIS by the Australian Criminal Intelligence Commission. The NCIS is intended to strengthen criminal information and intelligence sharing across law enforcement agencies, jurisdictions

[1] Some of the recommendations made in this submission are compatible with the recommendations of the 2017 Independent Intelligence Review, in particular the recommendation that a comprehensive review of the Acts governing Australia's intelligence community should be undertaken to ensure that agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians (recommendation 15).

and the criminal intelligence community and to offer enhanced digital analytical and collaboration services. The project included doctrinal analysis of federal and state legislation, interviews with users of the NCIS pilot, including senior police officials.

The project found that one of primary challenges to implementation of the NCIS was an outdated and overly complex legislative framework. Much of the problem emanates from the fact that current legislation concerning information sharing amongst law enforcement agencies in Australia is outdated not only in terms of technology currently used by law enforcement agencies but also in terms of future technological developments. It uses outdated terminology and concepts, and as a result places arbitrary restrictions on information use and sharing which impede information sharing.

The most significant of these outdated concepts is use of property concepts to describe the relationship between entities and information. In particular, in the context of cloud computing and shared data platforms, it is not clear what it means to 'hold', 'own' or 'possess' information. Inappropriate terminology adds a layer of confusion and uncertainty in relation to the NCIS and similar information sharing models. Recommendations 1 - 4 draw specifically on this project.

b) The second project completed by the Law and Policy program examined data governance structures associated with the NCIS. The project, titled *A Governance Framework for Law Enforcement Information Sharing under the National Criminal Intelligence System* investigated governance structures, including information governance structures, for the NCIS. The project was informed by a workshop with officials from the Australian Criminal Intelligence Commission and analysis of laws and policy documents relating to the Commission and the NCIS. The project also included a survey of Compliance by Design approaches and research internationally. Recommendation 5 draws specifically on this project.

c) The Law and Policy Program is currently undertaking a third research project, titled *Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement*. This project examines the use of open source data and information by law enforcement, defence and national security agencies for designated purposes, and focuses especially on the analysis of social media. Participating agencies are the Australian Federal Police, the Attorney-General's Department, the Department of Immigration and Border Protection, and the Queensland Police. The project will conclude in September 2018. The initial phase of the project has included an extensive literature review and a workshop with participating agencies, which have highlighted several issues concerning challenges facing Australia's law enforcement agencies arising from new and emerging ICT. Recommendations 6 and 7 draw specifically on initial findings from this project, which is still in its preliminary stages.

Recommendations

The recommendations relate to the committee's terms of reference (ToRs). Recommendations 1 – 7 relate to ToR A (Challenges facing Australian law enforcement agencies arising from new and emerging ICT) while recommendations 6 and 7 relate to ToR B (The ICT capabilities of Australian law enforcement agencies).

1. In the long term, the legal framework for information sharing could be simplified by bringing disparate laws together in one place rather than amending different pieces of legislation (ToR A). [2] This could mean a single Commonwealth Act containing rules for how and when Commonwealth data is collected, distributed, accessed, used, stored and deleted, accounting for—among other issues—changes in technology since the original legislation was drafted. Such an Act could preserve some distinctions for specific data sets or agencies (based on differential risk), but 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 any such new law.

2. In consultation with parliamentary counsel, Government should consider developing consistent and comprehensive definitions that clarify core information concepts in a digital age in order to begin a process of standardising and updating legislative terminology around access to, use of and disclosure of data within and among Commonwealth, State and Territory entities (ToR A). [3] These concepts are addressed in the recommendations below[4].

2.1 Government should consider updating and simplifying terminology and concepts relating to the concept of data ownership in relevant legislation (ToR A). [5] The idea of "data ownership" or "possession of data" is confusing and unhelpful in a digital age. The concepts of data ownership, at present (inconsistently) defined in state and federal legislation, draw on outdated notions of data ownership which link ownership and responsibility to the idea of physical property. This means that a range of legislation dealing with information sharing in a law enforcement context currently treats information as if it can only be held by one person at one time. This approach cannot account for the myriad of ways in which digital information can be used, copied, shared and stored. In future,

[2] Recommendation based on research completed for the project 'Information sharing and the National Criminal Intelligence System (NCIS)', completed in August 2017.
[3] Recommendation based on research completed for the project 'Information sharing and the National Criminal Intelligence System (NCIS)', completed in August 2017.
[4] Recommendations concerning the clarity of terminology and definitions echo recommendation 15 in the 2017 National Independent Intelligence Review.
[5] Recommendation based on research completed for the project 'Information sharing and the National Criminal Intelligence System (NCIS)', completed in August 2017.

legislative drafters should avoid property language in linking information and electronic documents to agencies and, over time, it should be removed from existing statutes. Legislation, including in relation to 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).

2.2. Government should consider updating and simplifying terminology and concepts relating to restrictions on disclosure in relevant legislation (ToR A).[6] 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. Current legislative framing of disclosure and use assume a simplistic model of information sharing that does not take account of automated means of sharing (such as shared data platforms). Managing disclosure risks should not rely so heavily on control of information being allocated to a particular agency, particularly where disclosure occurs between Commonwealth agencies, but also where it occurs between Commonwealth and State or Territory agencies. Information governance should rely on a combination of use and disclosure restrictions that recognise the government's policy that data be treated as a "national asset" and thus not unnecessarily restricted to a single agency.

3. Government should pursue a consistent principles-based approach to information sharing between law enforcement agencies (ToR A).[7] Both Commonwealth and State laws are drafted around specific rules for disclosing data in particular databases or specific rules for specific agencies (concerning what data they can access and/or what data they can disclose). The authorising Act for an agency will generally contain some specific provisions about access to and disclosure of data for that agency, which often combine with the data specific legislation where that applies. At present, largely because of developments in technology and changes in the way information is used, references to data disclosure in these types of legislation do not adequately reflect the range of data available to users or the ways in which it may be stored, used or shared and can inhibit information sharing between law enforcement agencies. Such legislation also operates in addition to the Protective Security Policy Framework, which is compulsory at the Commonwealth level and adopted voluntarily by some states and territories.

[6] Recommendation based on research completed for the project 'Information sharing and the National Criminal Intelligence System (NCIS)', completed in August 2017.
[7] Recommendation based on research completed for the project 'Information sharing and the National Criminal Intelligence System (NCIS)', completed in August 2017.

A consistent approach should be pursued across the Commonwealth, States, Territories to ensure seamless information sharing, where appropriate. 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 (see recommendation 5).

4. Government should also pursue a consistent risk-based approach to information sharing between law enforcement agencies (ToR A).[8] Currently, legislation assumes that rules and restrictions on information should apply to an entire law enforcement database or agency, despite variation in the sensitivity of information and risk profile associated with disclosure within a single dataset or within data in the control of a single agency. New technologies combined with Compliance by Design and Compliance through Design approaches mean that a more fine-grained and risk-based approach is feasible. 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.

5. Government should consider assessing the data governance capabilities of senior management of national security and law enforcement agencies and providing appropriate support to those who are accountable for data governance (ToR A).[9] The complexity of enhanced data analytical capabilities presents governance challenges for government agencies dealing in data flows enhanced and driven by new technologies. Care should be taken to ensure that governance structures of the relevant agencies have the necessary technical expertise to govern the opportunities and risks presented by enhanced data analytical capabilities. It would be advisable to assess the data governance structures and capabilities of each agency and, where required, ensure that good data governance is supported with training and human resources. In some cases an agency may benefit from the establishment of a technical advisory committee that can provide its governance structures with independent, technical advice on risks and opportunities presented by new technologies as well as technologies employed by the agency.

[8] Recommendation based on research completed for the project 'Information sharing and the National Criminal Intelligence System (NCIS)', completed in August 2017.

[9] Recommendation based on research completed for the project, 'A governance framework for law enforcement information sharing under the National Criminal Intelligence System' (project completed in June 2017).

6. Government should consider using processes associated with the Budapest Convention or other measures to address the inadequacy of MLAT processes for Australian law enforcement purposes (ToR A, ToR B).[10] Like law enforcement agencies elsewhere, Australian law enforcement agencies rely on the Mutual Legal Assistance Treaty (MLAT) process to access information from social media companies which they may need to effect a persecution. In Australia, the *Evidence Act 1995* (Cth) encourages law enforcement agencies to liaise with social media companies to produce the required format of this information for use in court, meaning Australia is possibly at a comparative disadvantage to other states which may not have to manage this requirement. However, the MLAT process is universally agreed to be inefficient and slow and does not meet the needs of law enforcement agencies globally. The average waiting time for Australian law enforcement agencies for a response from foreign social media companies is often a minimum of 6-12 months. Additionally, the MLAT process does not facilitate Australian law enforcement access to social media data for threat identification purposes or other uses which are not attached to either an offence or a trial. Australia is a signatory to the Budapest Convention on Cybercrime, which facilitates the MLAT process. The US and the UK have negotiated a draft agreement, not publicly available, which appears designed to take the place of MLAT process agreements. This agreement follows the UK's appointment of a special envoy on intelligence and law enforcement data sharing to the US in 2014. Australia should be engaged in this and other efforts to further improve and update the MLAT process.

7. Government should examine mechanisms for increasing language abilities in law enforcement agencies for access to non-English -language social media. It should also engage with non-English language social media companies to facilitate access to material by law enforcement agencies (ToR A, ToR B).[11] Individuals of interest to Australian law enforcement agencies use a range of non-English language social media and chat applications which are not easily accessible to these agencies. WeChat, for example, is a chat application owned by Chinese technology giant Tencent, and Australia now has approximately three million WeChat users.[12] Our discussions suggest Australian agencies are likely to have difficulty accessing this material and material from other non-English language applications because of language barriers and also because there is no formal government liaison relationship with WeChat or other technology/social media companies with a non-English speaking

[10] Recommendation from preliminary research as part of the project 'Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement' (project underway, due to be completed in September 2018). This recommendation echoes recommendations 13 and 14 of the 2017 Independent Intelligence Review.

[11] Recommendation from preliminary research conducted as part of the project 'Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement' (project underway, due to be completed in September 2018).

[12] Lv, L. (2017) Who are the Australians Using China's WeChat? https://www.sbs.com.au/yourlanguage/mandarin/en/article/2017/11/01/who-are-australians-are-using-chinas-wechat (2017) (accessed 01/01/18)

background. There is a formal government liaison relationship with similar English-language driven technology/social media companies such as Facebook and Google through the Digital Industry Group Incorporated (DIGI) .

References

D2D CRC Law and Policy Projects

Associate Professor Lyria Bennett Moses (UNSW Law), Professor Janet Chan (UNSW Law), Dr Alana Maurushat (UNSW Law), Dr Sarah Logan (UNSW Law), *Information sharing and the National Criminal Intelligence System (NCIS)* (2017)

Associate Professor Lyria Bennett Moses (UNSW Law), Professor Janet Chan (UNSW Law), Dr Sarah Logan (UNSW Law) *Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement* (ongoing, to be completed September 2018).

Professor Louis De Koker (La Trobe), Adjunct Professor David Watts (La Trobe, Office of the Victorian Commissioner for Privacy and Data Protection), Professor Pompeu Casanovas (La Trobe), Associate Professor Sara Smyth (La Trobe), Dr Bridget Bainbridge (La Trobe), *A Governance Framework for Law Enforcement Information Sharing under the National Criminal Intelligence System* (2017)

D2D CRC Law and Policy Reports

Associate Professor Lyria Bennett Moses, (UNSW Law), *Final Report, Information Sharing and the National Criminal Intelligence System (NCIS)* D2D CRC Law and Policy Program (2017)

Dr Sarah Logan (UNSW Law), Associate Professor Lyria Bennett Moses (UNSW Law), *Post-Workshop Paper, Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement* (2017)

Adjunct Professor David Watts (La Trobe, Office of the Victorian Commissioner for Privacy and Data Protection), Professor Louis de Koker (La Trobe); Dr Bridget Bainbridge (La Trobe), Professor Pompeu Casanovas (La Trobe), Associate Professor Sara Smythe (La Trobe) *A Governance Framework for the National Criminal Intelligence System (NCIS)* D2D CRC Law and Policy Program (2017)

Articles and Reports

Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review* (2017)

Lucy Lv, Who are the Australians Using China's WeChat? https://www.sbs.com.au/yourlanguage/mandarin/en/article/2017/11/01/who-are-australians-are-using-chinas-wechat (2017) (accessed 01/01/18)