OPEN SECRETS: BALANCING OPERATIONAL SECRECY AND TRANSPARENCY IN THE COLLECTION AND USE OF DATA BY NATIONAL SECURITY AND LAW ENFORCEMENT AGENCIES

LYRIA BENNETT MOSES* AND LOUIS DE KOKER†

In a world where analysis of large volumes of data can predict what people will read, watch and buy, governments are increasingly under internal and external pressure to predict events which threaten national security. Data analytics promises to be a powerful tool for governments seeking to identify and disrupt threats, better understand criminal networks and improve strategic decision-making. Because these tools raise public concerns, there needs to be a sufficient degree of transparency and openness in order to support meaningful public debate and individual rights. However, the barriers to greater transparency include the need for operational secrecy, commercial confidentiality of the analytic tools themselves and the challenges of rendering accessible complex algorithms with emergent properties. This article draws on doctrinal and empirical elements of a comparative study of strategy, law and policy around the use of Big Data technology for national security and law enforcement agencies in order to explore these tensions. In particular, we ask how Australia might enhance transparency in relation to the collection, access and use of data for national security and law enforcement purposes. It is argued that clear powers, subjected to open public debate, with sufficiently resourced oversight of agency processes and some public 'translucency' as to algorithms and methods are the best means of ensuring a socially acceptable approach to data-driven decision-making by national security and law enforcement agencies.

* BSc (Hons), LLB (UNSW), LLM, JSD (Columbia); Director, Allens Hub for Technology, Law and Innovation; Associate Professor, Faculty of Law, UNSW Sydney; Project Leader and Key Researcher, Law and Policy Program of the Data to Decisions Cooperative Research Centre ('Data to Decisions CRC').

† BIuris, LLB, LLM, LLD (University of the Free State), LLM (Cantab); Professor, La Trobe Law School, La Trobe University; Program Lead, Law and Policy Program of the Data to Decisions CRC. We would like to express our thanks to Linly Wang for research assistance, and to the anonymous reviewers for their helpful feedback. All remaining errors are our own. Data to Decisions CRC funding is acknowledged but the views expressed are not necessarily reflective of the views of the centre or any of its members.

Cite as:

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* (advance)

Contents

I Introduction

In a world where analysis of large volumes of data can predict what people will read, watch and buy, governments are increasingly under internal and external pressure to predict events which threaten national security. Data analytics promises to be a powerful tool for governments seeking to identify and disrupt threats, better understand criminal networks and improve strategic decision-making. However, the possibility of governments using increasingly powerful tools to analyse large volumes of citizen-generated data gives rise to concerns about the implications of state surveillance for privacy and free speech. There are important choices for democratic societies to make about the circumstances in which citizen data ought to be collected, accessed, analysed and acted upon by national security and law enforcement ('NSLE') agencies. Once the parameters are set, the effect and impact of the systems must be monitored to ensure that the actual benefits outweigh the risks.

In order to support meaningful democratic debates on these issues, there needs to be a sufficient degree of transparency and openness. Drawing the lines between what should be known and what should be hidden in relation to NSLE is traditionally complex and controversial. In the context of NSLE operations,

there is a legitimate need for secrecy, but there are dangers as well in cultures of secrecy and incentives for secrecy that extend beyond this strategic need.[1] In addition to this historic tension, new analytical techniques create additional challenges for transparency, linked for example to their inherent complexity.

This article will explore these tensions in two contexts — the need for clear, transparent government powers concerning the collection, access and use of citizen data, and the need for some understanding and oversight of the processes and algorithms used to draw inferences about individuals or groups that drive agency decision-making. It is argued that clear powers, subjected to open public debate, with sufficiently resourced oversight of agency processes and some public 'translucency' as to algorithms and methods are the best means of ensuring a socially acceptable approach to data-driven decision-making by NSLE agencies in Australia.

This article draws on doctrinal and empirical elements of a comparative study of strategy, law and policy around the use of Big Data technology for NSLE agencies.[2] The empirical component of the study comprised semi-structured interviews with operational, technical and policy stakeholders in Australia and the United Kingdom. The design of the empirical inquiry acknowledged the contingency and variability of technological design and practices.[3] In order to meaningfully explore, contextualise and map differences and agreements in the policy, laws and risk assessment and compliance practices in different jurisdictions and organisations, differences in 'technological frames' (being assumptions, expectations and knowledge about a technology) were taken into account.[4] We focused primarily on Australian stakeholders, given the objective of the project was to make recommendations for Australia.

Interviews were conducted with key stakeholders, technologists and users in each country in relation to their understanding of the capabilities, uses and

[1] This issue is not new: see, eg, Carl J Friedrich, 'Some Observations on Weber's Analysis of Bureaucracy' in Robert K Merton et al (eds), *Reader in Bureaucracy* (Free Press, 1952) 27, 29; Joseph E Stiglitz, 'On Liberty, the Right to Know, and Public Discourse: The Role of Transparency in Public Life' in Matthew J Gibney (ed), *Globalizing Rights: The Oxford Amnesty Lectures 1999* (Oxford University Press, 2003) 115.

[2] The project, *Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law*, was funded by the Data to Decisions CRC.

[3] Lyria Bennett Moses, 'Bridging Distances in Approach: Sharing Ideas about Technology Regulation' in Ronald Leenes and Eleni Kosta (eds), *Bridging Distances in Technology and Regulation* (Wolf Legal Publishers, 2013) 37.

[4] Wanda J Orlikowski and Debra C Gash, 'Technological Frames: Making Sense of Information Technology in Organizations' (1994) 12 *ACM Transactions on Information Systems* 174. See generally Wiebe E Bijker, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (MIT Press, 1995); Janet BL Chan, 'The Technological Game: How Information Technology is Transforming Police Practice' (2001) 1 *Criminal Justice* 139.

risks of Big Data and related tools, their perception of issues and challenges in relation to Big Data and data access and sharing, their perception of existing and proposed strategies, policies, laws and practices, and their recommended responses to perceived challenges. Interviews were conducted face-to-face where possible and via Skype or videoconferencing where feasible. A total of 52 Australian and UK research participants took part in the research project: 38 from Australia (interviewed from 25 March 2015 to 13 November 2015) and 14 from the UK (interviewed from 24 February 2016 to 18 March 2016). These were based on responses to 74 invitations in Australia (51% participation) and 36 invitations in the UK (39% participation). Research participants covered a range of stakeholders including law enforcement and intelligence officials, oversight officials, policymakers, computer technologists (for the Australian study) and representatives of citizen groups. Participants in Australian law enforcement, national security and policy agencies were initially selected from a list compiled by our research liaison officials at the Attorney-General's Department based on role descriptions, and supplemented through referrals from those contacted or interviewed. For the Australian component, the Secretary of the Attorney-General's Department assisted by sending letters to the relevant agency heads endorsing the research project and suggesting that they encourage their staff to participate in the project when invited. Participants in the equivalent agencies in the UK were recruited with the assistance of the Australian Department of Foreign Affairs and Trade as well as Australian partner agencies. Participants from oversight agencies and citizen groups were selected by the research team, based on our reading of the legislative framework and our own research, respectively. Participants from technology companies with offices in Australia were selected in discussion with the management at the Data to Decisions Cooperative Research Centre. All participants spoke from their own experience, articulating their own views and perceptions (which may not be based on a comprehensive or accurate understanding of the issues involved), rather than as representatives of an organisational position. Quotations from interviews are intended to be indicative, rather than representative, of the views of the relevant populations of stakeholders in Australia and the UK.

Research participants were classified in accordance with their role and the nature of the organisation for which they worked. In each case, there were three potential classifications: Operational ('O'), Technical ('T') and Policy ('P'). The policy classification was broad, and included individuals and agencies with a legal or policy role, community organisations and NGOs and individuals and agencies with an oversight role over operational agencies. Where a research participant was being interviewed in relation to a recent former role, the coding

matched the former role and organisation rather than current role and organisation. Joint roles are recognised through hyphenation (eg 'O-P'). Because the technology companies in the T category were often international in scope, the UK interviews were limited to the O and P classifications. Overall, Australian participants belonged to organisations classified as 19 O, 7 T and 12 P; the UK participants belonged to 5 O and 9 P. Throughout this article, comments or quotes from interviews are identified with a 'role/organisation' classification (eg 'T/O'). We had three sets of overlapping questions that we used in the interviews. We labelled these 'Operational', 'Technical' and 'Policy'. The questions that research participants were asked generally aligned with their role and/or organisation, depending on the confidence of the participant with different types of questions. Although interviewers used a standard set of questions, there was some variation between interviews, which were semi-structured to allow a natural conversation between researchers and participants. Some interviews took place in small groups of two to three participants from the same organisation.

The perspectives gleaned from the empirical study combine with discussions in the literature and analysis from the legal position in both countries to explore how Australia might improve its transparency in relation to the collection, access and use of data for NSLE purposes.

II Transparency, Openness and NSLE Agencies

The importance of clarity and transparency in the scope of government powers has been proclaimed by a wide variety of well-known historical figures and theorists, including Milton,[5] Madison,[6] Mill,[7] Bentham,[8] Fuller,[9] and Stiglitz.[10] As a concept, transparency has been given different meanings and emphases.[11] For purposes of public accountability, transparency can be described as the 'availability of information about an actor allowing other actors to monitor the workings or performance of this actor'.[12] Transparency has also been defined as 'government according to fixed and published rules, on the basis of information and procedures that are accessible to the public'.[13] This latter definition is the one we adopt in this article, although we note that accessibility is not simply a question of publication, but also clarity and comprehensibility.[14]

[5] John Milton, *Areopagitica*, ed John W Hales (Oxford University Press, 1944). '[W]ho ever knew Truth put to the wors in a free and open encounter?': at 52.

[6] James Madison, *Letters and Other Writings of James Madison Fourth President of the United States: 1816–1828* (JB Lippincott & Co, 1867) vol 3, 276: 'A popular Government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or, perhaps, both. Knowledge will forever govern ignorance; and a people who mean to be their own governors must arm themselves with the power which knowledge gives.'

[7] John Stuart Mill, *Considerations on Representative Government* (Parker, Son, and Bourne, 1861) 109–10: 'As between one form of popular government and another, the advantage in this respect lies with that which most widely diffuses the exercise of public functions … by opening to all classes of private citizens, so far as is consistent with other equally important objects … and above all, by the utmost possible publicity and liberty of discussion, whereby not merely a few individuals in succession, but the whole public, are made, to a certain extent, participants in the government, and sharers in the instruction and mental exercise derived from it.'

[8] Jeremy Bentham, *The Theory of Legislation*, ed CK Ogden, tr Richard Hildreth (Routledge & Kegan Paul, 1931) 410–12.

[9] Publicity and clarity of laws were components of Fuller's eight principles of legality: Lon L Fuller, *The Morality of Law* (Yale University Press, 1964) ch 2.

[10] Stiglitz (n 1) 116: 'there should be a strong presumption in favour of transparency and openness in government'.

[11] Christopher Hood, 'Transparency in Historical Perspective' in Christopher Hood and David Heald (eds), *Transparency: The Key to Better Governance?* (Oxford University Press, 2006) 3.

[12] Albert Meijer, 'Transparency' in Mark Bovens, Robert E Goodin and Thomas Schillemans (eds), *The Oxford Handbook of Public Accountability* (Oxford University Press, 2014) 507, 511 (emphasis omitted).

[13] Christopher C Hood, 'Transparency' in Paul Barry Clarke and Joe Foweraker (eds), *Encyclopedia of Democratic Thought* (Routledge, 2001) 700, 701.

[14] Larsson has argued that the term 'transparency' is different to 'openness' in that it incorporates requirements of coherence, simplicity and comprehensibility: Torbjörn Larsson, 'How Open Can a Government Be? The Swedish Experience' in Veerle Deckmyn and Ian Thomson (eds),

Within government, transparency supports appropriate coordination, management and governance, and it is 'a key component of public policy effectiveness and efficiency'.[15] Public transparency provides the public with sufficient information regarding the exercise of powers and the managerial, political and independent oversight of the exercise of those powers to hold government accountable for its actions. Transparency is thus a necessary, but not sufficient, condition for accountability.[16] In addition to supporting accountable governance, public transparency has also been said to reduce the power of special interests, limit public corruption, incentivise the government to serve the interests of its citizens and reduce inefficiencies in transfers of power following elections.[17]

There are some important critiques of transparency as an ideal. While O'Neill has argued that transparency and accountability do not themselves produce public trust, her concerns are with poor metrics, lack of opportunity to exercise independent judgment, and information overload.[18] She does not discuss the need for clear, transparent grants of power to government agencies or challenge the need for human oversight of computer-driven processes. Her primary concern, that provision of information is often less useful than active inquiry and engagement,[19] is one that we share. Hood has also pointed out the limitations of the concept of 'transparency'.[20] Of particular importance here is his observation that it can conflict with other goals, such as the need for official secrecy.[21] Another critique comes from Ananny and Crawford, who argue inter alia that transparency can be ineffective at achieving accountability and that it

Openness and Transparency in the European Union (European Institute of Public Administration, 1998) 39, 40–2.

15 Ann Florini, 'Introduction: The Battle over Transparency' in Ann Florini (ed), *The Right to Know: Transparency for an Open World* (Columbia University Press, 2007) 1, 2. See also Alasdair Roberts, 'Transparency in the Security Sector' in Ann Florini (ed), *The Right to Know: Transparency for an Open World* (Columbia University Press, 2007) 309, 321–3.

16 Jonathan Fox, 'The Uncertain Relationship between Transparency and Accountability' (2007) 17 *Development in Practice* 663, 665. Some would argue that transparency is not important in itself, but it is only useful insofar as it serves the interests of accountability: Dennis Broeders et al, 'Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and the Use of Big Data' (2017) 33 *Computer Law and Security Review* 309, 319.

17 See Fox (n 16) 666. Transparent and clear laws are also crucial so that people are aware of what is required of them and what they might be subjected to: see, eg, Fuller (n 9) 49–51, 63–5.

18 See Onora O'Neill, *A Question of Trust: The BBC Reith Lectures 2002* (Cambridge University Press, 2002).

19 See ibid.

20 Hood (n 13) 703–4.

21 Ibid 704.

can itself cause harms (such as to individual privacy).[22] They prefer to look at system-wide accountability that recognises the limits of making any particular component of the system transparent. However, while this argument succeeds in demonstrating the centrality of accountability in determining what kinds of transparency are important, it cannot succeed without transparency. For example, the authors state that '[h]olding an assemblage accountable requires … understanding how it works as a system'.[23] Given that we define transparency in a way that incorporates clarity and comprehensibility, the point of the article, and one we agree with, is that transparency is not itself the end-goal, that it may conflict with other goals, and that it cannot guarantee system-wide accountability. This does not change the fact that, conversely, one cannot achieve accountability without a measure of transparency.

Australia is, generally speaking, committed to the idea of government transparency. Legislation such as the *Freedom of Information Act 1982* (Cth), the *Archives Act 1983* (Cth) and the *Public Interest Disclosure Act 2013* (Cth) promote government transparency in general. The *Privacy Act 1988* (Cth) also includes some transparency-promoting principles, albeit subject to exceptions that apply in NSLE contexts.[24] The Australian government formally expressed its intention to join the Open Government Partnership ('OGP') in May 2013,[25] and in November 2015 it committed to finalising its membership.[26] The Partnership is a multilateral government and civil society initiative 'established in 2011 that aims to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance'.[27] To qualify for membership a country must endorse a high-level 'Open Government Declaration', deliver a country action plan developed with public consultation, and commit to independent reporting on

[22] Mike Ananny and Kate Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2016) *New Media and Society* (forthcoming) 1.

[23] Ibid 11.

[24] See, eg, *Privacy Act 1988* (Cth) sch 1 ss 1, 5, 10, 12–13.

[25] Letter from Mark Dreyfus to Francis Maude, Kuntoro Mangkusubroto and Warren Krafchik, 22 May 2013 <www.opengovpartnership.org/documents/australia-letter-of-intent-join-ogp>, archived at <https://perma.cc/9UPX-RQA5>.

[26] Letter from Malcolm Turnbull to Open Government Partnership, 24 November 2015 <www.opengovpartnership.org/documents/australia-letter-of-intent-join-ogp>, archived at <https://perma.cc/UL4F-C6EL>.

[27] Australian Government, *Australia's First Open Government National Action Plan 2016–18: Draft for Consultation* (Draft Plan, 2016) 3 <https://ogpau.pmc.gov.au/sites/default/files/files/2016/10/Australias-first-Open-Government-National-Action-Plan-Draft-for-consultation-Accessible.pdf>, archived at <https://perma.cc/7C9Q-AM6G>.

their progress going forward.[28] Over seventy governments have made such commitments.[29] As part of the processes to finalise its membership, the government published *Australia's First Open Government National Action Plan 2016– 18* for consultation in late 2016, and is currently in the process of implementation.[30] Australia's membership of the OGP will further strengthen the government's commitment to greater access to information.

While the broader context to transparency and national security is relevant to this discussion, this article focuses on data and data analytics. Transparency around how the government collects, analyses and acts on data in the context of NSLE has historically been low. Agencies in some cases employed data practices that, even where legal, did not necessarily meet with large-scale public approval and threatened to undermine public trust in NSLE agencies.[31] This became clear after the June 2013 release of a cache of classified documents by Edward Snowden, a US employee of contractors for the US National Security Agency ('NSA').[32] The Snowden disclosures indicated that surveillance is not simply about spies in other countries, but about those who are not agents of any government who use the internet and phone services to communicate (O-P/O). The exposure of some secretive malware and hacking tools allegedly used by the NSA in August 2016 illustrates grounds for continuing concern.[33] The Snowden disclosures had particularly strong implications for all parties to

[28] Ibid 4; 'How to Join', *Open Government Partnership* (Web Page, 2017) <www.opengovpartnership.org/how-join>, archived at <https://perma.cc/MQ7Z-FW9Z>.

[29] 'About OGP', *Open Government Partnership* (Web Page) <www.opengovpartnership.org/about/about-ogp>, archived at <https://perma.cc/Q3RU-FGDD>. See also Australian Government, *Australia's First Open Government National Action Plan 2016–18* (n 27) 3.

[30] 'Australia's First National Action Plan Submitted', *Australian Government: Department of the Prime Minister and Cabinet* (Web Page, 7 December 2016) <https://ogpau.pmc.gov.au/2016/12/07/australias-first-national-action-plan-submitted>, archived at <https://perma.cc/8X6H-XAAN>.

[31] Royal United Services Institute for Defence and Security Studies, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (Whitehall Report No 2–15, July 2015) 34 ('*RUSI Report*') <https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf>, archived at <https://perma.cc/DCU9-X3H9>.

[32] Ibid 2 [0.7]; see also at 34 [2.19].

[33] Matt Burgess, 'Hacking the Hackers: Everything You Need to Know about Shadow Brokers' Attack on the NSA', *Wired* (San Francisco, 18 April 2017) <www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers>, archived at <https://perma.cc/E6FS-RZHE>.

the *United Kingdom–United States of America Agreement* ('Five Eyes'), including Australia.[34]

While transparency is crucial to sustain democratic controls over government, particularly in the context of data practices, it is also recognised that some aspects of government require a level of confidentiality or secrecy to support operational effectiveness. This is particularly relevant in relation to NSLE agencies. Where and how to draw the relevant lines between transparency and secrecy is, however, controversial. On the one hand, openness would compromise intelligence and operations to protect citizens or investigate crimes.[35] On the other hand, secrecy claimed is often broader than required,[36] so that secrecy said to be for the purposes of national security can hide serious abuses of power.[37] Secrecy, particularly as to the nature of government powers, how they are exercised and why they are justified also diminishes democratic accountability.[38]

To provide a measure of transparency where complete openness is not possible, audit mechanisms such as independent oversight bodies are employed. Functionaries such as the security-cleared Inspector-General of Intelligence and Security are empowered to investigate the actions of such agencies confidentially and report broadly but publicly on the outcomes of their investigations to Parliament and the public. These oversight bodies, if capable, independent and trusted by the public, serve as a proxy for the public in evaluating the conduct of necessarily secret operations.[39] While effective oversight agencies play a crucial role in enhancing accountability while maintaining operational secrecy, they are not a substitute for comprehensive public transparency where that is achievable.

[34] This five-country treaty involving the US, UK, Canada, Australia and New Zealand focuses on cooperation in signals intelligence: 'The Five Eyes', *Privacy International* (Web Page) <www.privacyinternational.org/node/51>, archived at <https://perma.cc/N6CT-GT9C>.

[35] Roberts (n 15) 314.

[36] See Carl J Friedrich, *Constitutional Government and Democracy: Theory and Practice in Europe and America* (Little, Brown and Co, 1941) 55; Dennis Broeders, 'The Secret in the Information Society' (2016) 29 *Philosophy and Technology* 293. See also the Queensland Council for Civil Liberties submission noted in Department of the Prime Minister and Cabinet, Commonwealth of Australia, *2017 Independent Intelligence Review* (Report, 2017) 122 [7.37] ('*2017 Independent Intelligence Review*') <www.pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf>, archived at <https://perma.cc/QJZ3-WELB>.

[37] Roberts (n 15) 314–16.

[38] Ibid 316–22.

[39] *2017 Independent Intelligence Review* (n 36) 111 [7.2].

There are thus three layers of transparency in the context of the data practices of NSLE agencies: within a NSLE agency, within an external oversight context and towards the general public. There are three dimensions of transparency with similarities and differences in terms of the impact on the different layers. The first, explored in Part II(A), is the extent of openness towards different layers and, in particular, the impact of operational secrecy and commercial confidentiality on the availability of information to the public. While some information can be justifiably withheld from disclosure, we argue that much of what is hidden (including the scope and nature of oversight processes and some information about data analytic methodologies) ought to be made public. The second, explored in Part II(B), is knowledge and understanding of the content of government data powers. The complexity of legislation and difficulties in interpretation is shared across the three layers while the limited availability of material to the general public has additional implications for public transparency. The third, explored in Part II(B), is the challenge of algorithmic transparency, with common challenges across layers (including the difficulties in understanding the behaviour of algorithms) as well as differences between them (in particular, as to access to technical expertise and operational secrecy concerning algorithms).

A *Views on Public Transparency of Powers to Collect, Access and Use Data*

The use of Big Data compounds concerns about the transparency of government powers. NSLE agencies are seeking access to more data about individuals (both citizens and non-citizens) in order to identify patterns and threats. There are divergent views on the extent to which such activities should be conducted given the intrusion on privacy, risk to data security and potential for abuse inherent in the collection of, access to and use of datasets containing personal information.[40] A public exploration of these views requires that the public know and understand the boundaries of government power in this context. The importance of public transparency regarding powers, capacity and general practices has been mentioned by the Executive Office of the President (US) in its

[40] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (Report, 1 May 2014) <https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>, archived at <https://perma.cc/R4RE-ZL2Y>. See also Stewart A Baker, *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism* (Hoover Institution Press, 2010) 313–14.

recommendation 'that the Administration should work to increase … transparency about intelligence practices where possible',[41] and in views expressed in UK reports informing the drafting of the *Investigatory Powers Act 2016* (UK).[42] Below, we highlight some themes that emerged among research participants in relation to the importance and limitations of public transparency, as well as what it might require in the context of NSLE data practices.

1 *Public Trust*

The importance of transparency and awareness around NSLE data powers was recognised in many of our interviews with Australian informants. For example:

> I think [the challenge] is probably around actually understanding primary and secondary use of data and … having a conversation across government around how actually we're going to manage that and explain it to the community (O-P/O).

Research participants also identified the connection between transparency and public acceptance and trust of NSLE agencies. This is a connection that has been noted in both the academic literature and the public service,[43] although the relationship is obviously complex, involving many other factors.[44] Public acceptance of the legal regime was particularly important because, as one participant responded, 'we police by consent' and 'we don't believe that [there is] public confidence in agencies to use … information wisely' (O/O). The idea of policing by consent stems from the so-called Peelian principles that continue to influence Australian law enforcement agencies such as the Australian Federal Police.[45] The Peelian principles link public trust with achievement of law enforcement goals.[46] The lack of public acceptance or trust in NSLE agencies was mentioned by 11 Australian participants working in organisational, policy and

[41] Ibid 79.

[42] See Part III.

[43] See, eg, Vivek Ramkumar and Elena Petkova, 'Transparency and Environmental Governance' in Ann Florini (ed), *The Right to Know: Transparency for an Open World* (Columbia University Press, 2007) 279, 283; Henry Belot, 'Public Servants Warned of Public Distrust', *The Canberra Times* (Canberra, 1 March 2016) 4.

[44] See, eg, Virginia A Chanley, Thomas J Rudolph and Wendy M Rahn, 'The Origins and Consequences of Public Trust in Government: A Time Series Analysis' (2000) 64 *Public Opinion Quarterly* 239.

[45] See Commissioner Andrew Colvin, 'Address to the Australian Intercultural Society' (Speech, Melbourne, 17 February 2016) <www.afp.gov.au/news-media/national-speeches/address-australian-intercultural-society>, archived at <https://perma.cc/CT2C-SM84>.

[46] Joseph A Schafer, 'The Role of Trust and Transparency in the Pursuit of Procedural and Organisational Justice' (2013) 8 *Journal of Policing, Intelligence and Counter Terrorism* 131, 131–2.

technical organisations as a barrier or challenge to the possibility of greater use of Big Data for NSLE purposes. This was described by two participants (P/P, T/T) as the 'biggest challenge'. Public trust is particularly important because much government data collection requires that 'people will voluntarily participate' (T/O).

2 *Transparency regarding Powers*

Most Australian research participants thus agreed that there should be transparency as to what datasets, or what types of datasets, could be collected and accessed. This is essentially transparency as to the scope of government power. One participant (O-P/O) went further, stating that transparency as to 'how they regulate and oversee their law enforcement and intelligence agencies' capability' was 'most important'. In other words, the scope of government power, *as well as regulation and oversight of that power*, need to be transparent.

Another strand of comments related to the reasons or purposes of government powers. Some Australian research participants emphasised that transparency needed to go beyond identifying the datasets that could be collected and accessed. For example, four participants (P/T, P/P, two O-P/O) mentioned the importance of being transparent about the *purposes* for which data was being used. Similarly, one UK participant (P/P) commented that, while the *Investigatory Powers Act* would ensure the public knew what data sets were accessed, '[w]e don't know hugely about how they're actually used' or 'why they're using them' which led to some concern that the 'actual operational case' for having access to the data remained obscure.[47] This relates to the question not merely of public transparency of the content of powers but also their justifications. It goes beyond the rule of law requirement for publicity of the content of law to a democratic requirement for the kind of understanding that can facilitate public debate and engagement.

3 *Impact of Transparency on Data Practices*

As well as engendering public trust, transparency has substantive advantages in ensuring appropriate and effective use of data. Transparency was described by Australian participants as important to 'match community values' (P/P), to

[47] This observation predated the investigation of the operational case for the exercise of bulk powers by the Independent Reviewer of Terrorism Legislation in relation to the *Data Retention and Investigatory Powers Act 2014* (UK), as repealed by *Investigatory Powers Act 2016* (UK) s 8(3): see David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Report, June 2015) 5 [14] ('*Anderson Report*') <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>, archived at <https://perma.cc/6D89-U7JE>. See the discussion in Part III.

'avoid abuse', given that silence about the 'grey zone' increases the risk of entering a 'black zone' (P/P), and to maintain public perceptions of Australia as something other than a 'police state' (P/P).

4 *Limits to Transparency*

While transparency as to government powers, rationales and practices is crucial, there are also reasons expressed by research participants as to why full transparency about data practices is problematic. Most crucially for many government participants, below a certain level of detail, information about data accessed, algorithms employed and processes relates to precisely the kind of operational capability that agencies are keenest to protect. In particular, there are concerns that criminals wishing to avoid attention might work around what they know about agency data collection and analysis.[48]

Increasing crime and terrorism concerns escalated the need for appropriate solutions. In Australia, for example, organised crime, the rise of the Islamic State ('IS') (also known as ISIL or Daesh), internal 'radicalisation', Australians joining foreign conflicts, a number of foiled plans for terrorist attacks on Australian soil and the Lindt Café siege are major drivers of the NSLE agenda.[49] A common concern raised by Australian research participants was the possibility that disclosure of what data was collected or accessed could reveal investigative techniques or methods (P/P, three O-P/O), a point also made by six UK research participants in the policy group. For example, one Australian research participant stated:

> Every time it appears in the press that … suspected terrorist X used a certain type of application to communicate and law enforcement were able to listen to it then they stop using it and then it puts us behind the eight ball again (O-P/O).

[48] See Tal Z Zarsky, 'Transparent Predictions' [2013] *University of Illinois Law Review* 1503, 1553– 8.

[49] See, eg, Australian Government: Department of the Prime Minister and Cabinet and NSW Government: Premier and Cabinet, *Martin Place Siege: Joint Commonwealth–New South Wales Review* (Report, January 2015) <www.pmc.gov.au/sites/default/files/publications/170215_Martin_Place_Siege_Review_1.pdf>, archived at <https://perma.cc/7PTD-U53A>; Australian Crime Commission, *Organised Crime in Australia 2015* (Report, May 2015) <https://www.acic.gov.au/sites/g/files/net1491/f/2016/06/oca2015.pdf?v=1467241691>, archived at <https://perma.cc/C6DU-3PCG>; Australian Security Intelligence Organisation, *ASIO Annual Report 2015–16* (Annual Report, 27 September 2016) 17–19 <www.asio.gov.au/sites/default/files/2016%20ASIO%20Annual%20Report%20UNCLASSIFIED.pdf>, archived at <https://perma.cc/8KVT-AJN4>; 'Fighting Terrorism Overseas', *Australian Federal Police* (Web Page) <www.afp.gov.au/what-we-do/crime-types/fighting-terrorism/fighting-terrorism-overseas>, archived at <https://perma.cc/K9MG-DQ6D>.

This is similar to the point made by one UK participant that the type of data collected 'is part of their methods' (P/P).

This concern does not necessarily imply that there should be *no* transparency, but it does raise the question of whether there could be a degree of breadth in the disclosure that preserves public input into the scope of agency powers, while avoiding making disclosures that reveal a capability (O-P/O). As one participant noted, there is a 'balance' where disclosure should occur if it does not 'cause issues' (P/P). One suggestion (P/P) is that one disclose the 'envelope', namely the data that could in principle be collected and accessed by government, including, within this list, data that is not actually collected or accessed, perhaps because it is not technologically or practically possible to do so.

The Australian and UK interviews revealed similar themes in terms of the importance and limits of public transparency around collection of and access to data for NSLE purposes. The difference between the two countries lies in the fact that Australia has not undertaken a large-scale review and consolidation of its laws concerning NSLE agency access to and use of data. The UK, as discussed in Part III, has done so.

5 *Worrying Rationale against Transparency*

While there can be controversy over the precise boundaries of operational secrecy in the context of data powers, there was one Australian participant who raised a more troubling rationale for secrecy. This participant (O-P/O) mentioned that it could 'open up exposure' to public critique. The Snowden revelations, for example, opened up public debate about whether surveillance on a large scale was warranted in light of the security threat.

The challenge in this case is that a political debate about data powers may not be sufficiently informed and may put at risk powers that should be available to be exercised under appropriate conditions. However, while the public debate regarding the Snowden revelations was not necessarily sufficiently informed, and may have had results that did not enjoy the support of more conservative security proponents, a democratic society should create space for appropriate debate. Such debate might prove fruitful in facilitating a better understanding of the seemingly incongruent positions taken in opinion polling.[50] If the concern is that uninformed debate may threaten appropriate powers, ways should be found to inform the debate, particularly as to safeguards and oversight.

[50] See, eg, George Gao, 'What Americans Think about NSA Surveillance, National Security and Privacy', *Fact Tank: News in the Numbers, Pew Research Center* (Online, 29 May 2015) <www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/>, archived at <https://perma.cc/PCB9-2EH4>.

While the public cannot have a *fully* informed debate — the nature of operational capabilities and hence the extent to which operational capabilities trail agency powers would remain secret — it is submitted that the debate can and should be about what powers are *granted and when they may be exercised*, not what powers are *used* in specific cases.

B *Transparency of Data Collection and Access Powers in Australia*

Australia has a complex set of laws that governs when and how agencies can collect and access data. A prominent example is the power under the *Telecommunications (Interception and Access) Act 1979* (Cth) to require telecommunications providers to retain telecommunications metadata so that it can be accessed in the course of NSLE inquiries.[51] There are also mechanisms that allow state police forces to share data relevant to criminal investigations, originally through CrimTrac and now, since 2016, through the Australian Criminal Intelligence Commission.[52] However, there has not been wholesale reform of the complex network of laws, regulations, memoranda of understanding and internal rules that control how NSLE agencies access and use data. The number and diversity of sources of partial information on data access and general management of data by government agencies for NSLE purposes pose a transparency challenge to the extent they make it difficult to understand the actual scope of

[51] *Telecommunications (Interception and Access) Act 1979* (Cth) pt 5-1A, as amended by *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) sch 1 pt 1.

[52] See generally Michael Keenan, 'New Super Agency to Tackle Emerging Threats' (Media Release, 5 November 2015).

government powers.[53] Even though there is some publicly available information (in particular, those laws enacted by Parliament), this '[o]paque … transparency'[54] does not reveal how government powers operate in practice.

The complexity of Australia's legislative framework as to the circumstances in which data can be shared was raised by some research participants. The legislative framework was described as 'complex' (T/O), with one participant noting that there is not a 'common legal view' as to the ownership of data held by government agencies. Some complexity also arises from the fact that 'each state has its own regime' (O-P/O). As a result of this complexity, it was often unclear even *within* government whether information could be shared, with some agencies concerned that legal barriers were being used as a false excuse not to share data, for example:

> There's also inconsistent understanding and views of privacy laws. So different agencies will take a particular interpretation of personal data or privacy and can put up artificial barriers or misunderstanding when it comes to us accessing it under the *Privacy Act* (O/O).

The problem is potentially greater when it comes to the understanding of the scope of agency powers and oversight mechanisms by those outside government. This was evident in the responses of research participants to a question asking them to identify laws, regulations and procedures governing the use of

[53] Information sources include parliamentary debates, evidence and reports, for example those stemming from the work of the Parliamentary Joint Committee on Intelligence and Security (see, eg, Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, 27 February 2015) <www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report>, archived at <https://perma.cc/4UKP-2RSJ>) and annual reports by NSLE agencies and oversight bodies. In the case of intelligence agencies, the availability of such documents and reports is more limited. While the Australian Security Intelligence Organisation and the Inspector-General for Intelligence and Security produce annual reports that are tabled in Parliament, the Office of National Assessments and the Australian Secret Intelligence Service do not. The annual report of the Department of Defence includes only very general references to the activities of Defence intelligence agencies: see, eg, Department of Defence, Australian Government, *Defence Annual Report 2015–16: Volume One — Performance, Governance and Accountability* (Report, 2016) 42–4 <www.defence.gov.au/AnnualReports/15-16/Downloads/DAR_2015-16_Vol1.pdf>, archived at <https://perma.cc/K464-G6ZU>. A number of public government policy documents and operational documents (see, eg, Strategic Policy and Intelligence, Department of Defence, Australian Government, *2016 Australian Government Information Security Manual: Executive Companion* (Manual, 2016) <www.asd.gov.au/publications/Information_Security_Manual_2016_Exec_Companion.pdf>, archived at <https://perma.cc/G5N2-Z7XP>) and regulation impact assessments are also relevant but their availability in relation to NSLE agencies is limited.

[54] Fox (n 16) 667.

data and data analytics by NSLE agencies. While most participants were familiar with the *Privacy Act 1988* (Cth), participants from government and independent oversight agencies were far more likely to be familiar with agency-specific legislation, the *Archives Act 1983* (Cth) and internal documents or memoranda of understanding, which were rarely mentioned by participants in the private, research or NGO sectors.

Clear legislation and greater publicity about publicly available laws, regulations and procedures are only part of the problem. In many cases, in particular for internal documents and memoranda of understanding, important legal mechanisms that govern the sharing of data across agencies are not made public at all. Such inaccessible documents do not only concern the powers themselves, but also oversight mechanisms, reducing public transparency as to the operation of the system as a whole.

Seven Australian research participants felt that the information gap between the agencies and the general public impeded public debate to some extent. Participants in government observed that '[o]versight is better than can be explained publicly' (P/P) and that, for oversight, 'the detail is not there' in publicly available documents (O-P/O). Similarly, another observed that '[p]eople think that we can do things that we can't' (T/O). As another participant commented, grievance about data retention laws 'might drop away if there is more transparency about how often, for what purpose and how is it done' (P/P). The lack of public information inhibits public debate generally. Not only is it difficult to critique activities of which one is unaware or does not understand, it is impossible to be reassured by protections, limitations and oversight recorded in secret manuals and memoranda of understanding.

Government participants were concerned about public misunderstandings around the current legal regime. One government participant described the 'lack of communication' combined with 'lack of effort by the public to understand the law' and a media that wants 'to scare people about Big Data' (P/P). Another participant suggested that the public was often not aware of actual legislation and policy, in particular the role played by oversight:

> The oversight agencies do exist. We have a lot of infrastructure around preventing misuse of data and … police are prosecuted for this stuff. There are police officers in jail today for wrongdoing under the *TIA* [*Telecommunications (Interception and Access)*] *Act*. So this isn't some mythical regime that exists on paper but isn't enforced. But … for whatever reason, the public doesn't believe in it (P/P).

Whether or not these perceptions about public understandings are real, the belief in relative public ignorance presents a potential barrier for motivating

greater public engagement by government. However, greater clarity and availability of information regarding powers and oversight mechanisms is the only democratically justifiable solution to real or perceived public lack of understanding. To the extent that the legal framework is contained in public legislation, there are often difficulties of both awareness and interpretation. More problematically, many of the policy justifications and much practical detail essential to public understanding of both access powers and oversight are contained in non-public documents.

C *The Challenge of Algorithmic Transparency: Knowing How Data Is Used*

While Australia has limited transparency of powers to collect and access data, questions about transparency in the *use* of data are even more problematic. This is not solely an issue for data analytics — the ways in which 'small data' are used in the minds of human intelligence officers and investigators to draw links between individuals and events is typically very non-transparent and prone to cognitive bias.[55] Nevertheless, there are reasons to expect more from computers than from humans in this regard. Humans are required to account to superior officers as well as to oversight agencies; there is no equivalent for algorithms and complex, automated analytical processes. There is thus a risk that algorithmic errors and biases will remain undetected against a backdrop of presumed neutrality.

The idea of *algorithmic* transparency implies a right to know not only what powers the government has but also the manner of their exercise — not just what data is collected but how it is analysed and used in decision-making. This is similar to what one Australian participant described as public disclosure of 'what they're doing, how they're doing it' (O-P/O). Other Australian research participants (five P/P, but none in an operational agency) also expressed the view that algorithms used by NSLE agencies should be transparent, for reasons including accuracy and robustness. This view was also expressed in the UK; for example, 'the most important thing is they tell us exactly why they're useful and what tools they want to use and how they're going to be used' (P/P) and 'I think the public would like to know that there are protections against algorithms be-

[55] Committee of Privy Counsellors, *Review of Intelligence on Weapons of Mass Destruction* (House of Commons Paper No 898, Session 200304) 108–9 [440]–[445], 112–13 [456]–[459], 114 [464]; Matthew Herbert, 'The Intelligence Analyst as Epistemologist' (2006) 19 *International Journal of Intelligence and CounterIntelligence* 666; Uri Bar-Joseph and Rose McDermott, 'Change the Analyst and Not the System: A Different Approach to Intelligence Reform' (2008) 4 *Foreign Policy Analysis* 127; Mark Phythian, 'Intelligence Analysis Today and Tomorrow' (2009) 5(1) *Security Challenges* 67.

ing used in a discriminatory way. We'd probably like to know about the processes through which such algorithms and queries are generated' (P/P). Transparency is also an issue if algorithms are used as evidence, as one UK participant (P/P) noted, 'otherwise it makes it impossible for somebody to mount a defence, if they say "oh, well, the computer says it was you"'.

Outside the NSLE context, algorithmic transparency has been said to be an important component of 'due process' (or natural justice in Australia) where administrative decisions affecting individuals are based on algorithms.[56] It is also important as a protective measure to ensure decisions are fair and do not discriminate.[57] Full transparency would generally require access to the source code as well as, arguably, any data used in the operation of the algorithm (for example, training data in the context of machine learning).[58]

Independent of the context, algorithmic transparency is difficult to achieve. Burrell has identified three 'forms of opacity', being reasons why full transparency in this context is difficult.[59] The first is 'opacity as intentional corporate or state secrecy',[60] although the 'or' is generally an 'and' in the context of NSLE. Not only are there NSLE agency concerns about operational secrecy, but, where software is provided by private actors, there will also be contractual restrictions on what can be disclosed about the algorithms. An additional issue is the fact that an assessor will need access to both the machine learning algorithm *and the data on which it was trained* in order to predict its behaviour on any particular input. Data is likely to have a significant influence on the *operation* of the algorithm — if data is biased, then the algorithm will re-enact the same bias when applied to new data.[61] However, this data will typically be private personal

[56] Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249.

[57] See Frank Pasquale and Danielle Keats Citron, 'Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society' (2014) 89 *Washington Law Review* 1413, 1421 ('secrecy is a discriminator's best friend'). See also Association for Computing Machinery US Public Policy Council, 'Statement on Algorithmic Transparency and Accountability' (Statement, 12 January 2017) <www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf>, archived at <https://perma.cc/4TJW-X7W3>; The Royal Society, *Machine Learning: The Power and Promise of Computers that Learn by Example* (Report, April 2017) 93–4 ('*Royal Society Report*').

[58] See, eg, Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1, 13–14.

[59] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data and Society* 1.

[60] Ibid 1; see also at 3.

[61] Lyria Bennett Moses and Janet Chan, 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability' (2016) *Policing and Society* (forthcoming) 5.

information and thus not available to the general public. The second is 'technical illiteracy', the fact that most members of the public (and management) do not have sufficient expertise to understand, technically, what an algorithm is doing even if they are allowed to review the source code.[62] The third is opacity stemming from human limitations to understanding a complex algorithm in action, operating on large volumes of complex data.[63] The challenge reaches beyond a mere lack of access to information about the algorithm, its design processes and the data. The dilemma is that human observers are attempting to 'impose[] a process of human interpretive reasoning on a mathematical process of statistical optimization', subjecting machine thinking to human interpretation.[64] This anthropomorphic analysis is clearly fallible. The third form of opacity is not merely a practical challenge in facilitating transparency. It explains why transparency may itself be unhelpful to trained humans wishing to understand, and potentially challenge, inferences drawn from complex algorithms.

Within the NSLE context, the issue of state or operational secrecy regarding both data and analysis was the primary concern raised by research participants about algorithmic transparency. In particular, many participants were concerned that those with criminal intent could use information about algorithms and processes to commit crimes without raising flags. For example, if 'people can work out how the business rules work and stay under the radar … it would defeat the whole purpose' (P/T).

Research participants who objected to *public* algorithmic transparency generally supported the suggestion that there should be transparency within government, particularly within the relevant agencies and within oversight agencies. One limitation that was mentioned is that internal disclosure could not be absolute and should remain on a 'need to know' basis (P/P, O-P/O). As one participant observed, 'there are police officers who are today police officers and tomorrow will become members of the public and the day after that will become members of bikie gangs' (P/P).

However, there was only one objection by research participants to the suggestion of selected officials with relevant clearances within an agency and the relevant oversight body having full access to algorithms and systems. The objection, from a participant in an oversight role in the UK, was less about the principle of transparency and more about the process. In that participant's view (P/P), full access to systems would require expertise that would itself require a

[62] Burrell (n 59) 4.

[63] Ibid 5; see also at 10: 'When a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension. Machine optimizations based on training data do not naturally accord with human semantic explanations.'

[64] Ibid 9–10.

large increase in resources and would potentially reduce trust between oversight agencies and operational agencies. The better process, according to this participant and another participant in the same agency (P/P), was for systems-level checks (or quality assurance) to occur internally within the relevant agencies, with external oversight focusing on ensuring that agencies' checking procedures were sufficient.

Other concerns, such as the commercial nature of some of the algorithms being used, and the complex, technical nature of the content, were also mentioned by a few participants in Australia and the UK. For example,

> [t]he [user in the agency] won't understand all the inputs and mechanisms. There is an element of 'black-boxing', mitigated as much as we can (T/O, Australia).
>
> [A]nalytics can be quite complicated. Most, a lot of people, don't necessarily know exactly how they work (O-P/O, Australia).

The issues around algorithmic transparency apply in different ways to agencies, oversight bodies and the public. The first form of opacity in Burrell's taxonomy affects public transparency primarily, although there will also be those in agencies which are deemed to fall outside the 'need to know' circle. The second form of opacity mostly affects the public and oversight agencies, although technical expertise within agencies may also be concentrated and not shared by important decision makers. The third form of opacity was not raised in interviews, but will be important across all three layers where more sophisticated algorithms with emergent properties are used.

III The United Kingdom: A Transparency Shift

The cache of classified documents disclosed in June 2013 by Edward Snowden included a large number of documents relating to the tapping by the UK Government Communications Headquarters ('GCHQ') of fibre optic cables carrying important global communications.[65] Prior to the Snowden revelations, the scope of bulk data access powers granted to NSLE agencies in the UK was non-transparent. The fact that agencies interpreted s 8 of the *Regulation of Investigatory Powers Act 2000* (UK) to allow for the issuing of thematic warrants was,

[65] *RUSI Report* (n 31) 2 [0.7], 46–7 [3.7], 47 [3.10]. Despite these revelations and their impact on greater transparency through law reform in the UK, public trust in UK intelligence agencies remained relatively high. Steiger ascribes this to the positive establishment views of GCHQ: Stefan Steiger, 'The Unshaken Role of GCHQ: The British Cybersecurity Discourse after the Snowden Revelations' in Wolf J Schünemann and Max-Otto Baumann (eds), *Privacy, Data Protection and Cybersecurity in Europe* (Springer, 2017) 79, 79, 91.

for example, not publicly avowed until March 2015.[66] Similarly, the use of s 94 of the *Telecommunications Act 1984* (UK) to access bulk communications data was only avowed in November 2015. The drafting of the provisions themselves did not alert the public to their actual use. For example, s 94(1) of the *Telecommunications Act* was broad and vague:

> The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be requisite or expedient in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

In July 2016 the Interception of Communications Commissioner's Office published a report on s 94 directions.[67] The report highlighted the difficulties that arise when the statutory powers are operated 'in secret and without codified statutory procedures'.[68] The report noted, for example, the lack of record keeping requirements and appropriate measures to support oversight over the ways in which s 94 directions are given and used.[69] In October 2016 the Investigatory Powers Tribunal held in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* that the pre-avowal secretive bulk communication data and bulk personal datasets collection regime under s 94 did not comply with art 8 of the *European Convention on Human Rights*.[70]

[66] Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* (House of Commons Paper No 1075, Session 2014–15) ('*ISC Report*') 21 [42]–[45]; *Anderson Report* (n 47) 104 [6.42]. 'The use by the security and intelligence agencies of bulk personal datasets was publicly avowed only on 12 March 2015 when the ISC [Intelligence and Security Committee of Parliament] published its report. I had already been extensively briefed on their use at all three agencies, and was also aware that the ISCommr [Intelligence Services Commissioner] has, for several years, been reviewing the use of bulk personal datasets as part of his duties': at 139 [7.69] (citations omitted).

[67] Sir Stanley Burnton, *Report of the Interception of Communications Commissioner: Review of Directions Given under Section 94 of the Telecommunications Act (1984)* (House of Commons Paper No 33, Scottish Government Paper No 2016/67, Session 2016–17).

[68] Interception of Communications Commissioner's Office, 'Statement by the Interception of Communications Commissioner's Office (IOCCO) on the Publication of IOCCO's Review of Directions Given under Section 94 of the Telecommunications Act 1984' (Press Release, 7 July 2016). See also Burnton (n 67) 53 [11.11].

[69] Burnton (n 67) 53 [11.11].

[70] [2016] UKIPTrib 15_110-CH. See also *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).

However, the United Kingdom has recently rewritten its laws in a new *Investigatory Powers Act*, less to broaden the scope of existing powers than to ensure that those powers are clear and that applicable rules and controls are more consistent. The legislation generated significant public debate, with opponents labelling the measure the 'snooper's charter'.[71] Such opposition is itself evidence of success rather than failure in the context of transparency, as the debate about what is appropriate has been brought into the public sphere. While the *Investigatory Powers Act* remains controversial, a number of additional protections were added in response to criticism from the public, from parliamentary committees, from independent commentators and from members of Parliament. The process leading up to the Investigatory Powers Bill 2016 (UK) illustrates how the UK became more transparent in how NSLE agencies collect, access and use data, at least with respect to clarity and transparency around the grant of powers.

In April 2014 the Grand Chamber of the Court of Justice of the European Union, in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*,[72] declared the European Union's *Data Retention Directive*[73] invalid.[74] The *Directive* 'provided the legal basis for UK Regulations requiring service providers to retain communications data for law enforcement purposes'.[75] As a consequence of the case, the UK was under pressure to immediately adopt laws that would 'ensure that UK law enforcement and security and intelligence agencies' could continue 'to access the telecommunications data … need[ed] to investigate criminal activity and protect the public'.[76] To secure cross-party support enabling the fast adoption of the proposed statutory solution, the *Data Retention and Investigatory Powers Act 2014* (UK) was enacted.[77] It was agreed that the Act should provide for the Home Secretary to 'appoint the independent reviewer of terrorism legislation to review the operation and

[71] See, eg, James Titcomb, 'Snoopers' Charter Could "Weaken" Internet Security, Say Tech Giants', *The Daily Telegraph* (London, 8 January 2016) 8; Kevin Rawlinson, 'Spies Can Hack Every Device in Town under "Snooper's Charter"', *The Times* (London, 22 June 2016) 2.

[72] (C-293/12 and C-594/12) [2014] ECR 238.

[73] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54.

[74] *Digital Rights Ireland* (n 72). See also *Anderson Report* (n 47) 15 [1.4].

[75] *Anderson Report* (n 47) 15–16 [1.4] (citations omitted).

[76] Ibid 15 [1.1].

[77] Ibid.

regulation of investigatory powers'.[78] The 2015 report of the Independent Reviewer of Terrorism Legislation, David Anderson QC, entitled *A Question of Trust* ('*Anderson Report*') was the result of this arrangement.

The *Anderson Report* complemented two other reports. The first of these was a parliamentary inquiry launched in 2013 by the Intelligence and Security Committee of Parliament ('ISC'). It resulted in a March 2015 report entitled *Privacy and Security: A Modern and Transparent Legal Framework* ('*ISC Report*').[79] The second report was an independent review of UK surveillance practices, announced by the UK government in March 2014.[80] The government appointed the Royal United Services Institute for Defence and Security Studies ('RUSI'), with a broad-based review panel representing senior government, industry, civil society and parliamentary expertise to consider broader questions regarding surveillance.[81] These questions included advising 'on the legality, effectiveness and privacy implications of the UK surveillance programmes, particularly as revealed by the "Edward Snowden case"'; examining 'potential reforms to current surveillance practices, including additional protections against the misuse of personal data, and alternatives to the collection and retention of bulk data'; and to assess 'how law enforcement and intelligence capabilities can be maintained in the face of technological change, while respecting principles of proportionality, necessity and privacy'.[82] The independent surveillance review report, entitled *A Democratic Licence to Operate*, was published by RUSI in July 2015.[83]

In November 2015, the UK government presented the draft Investigatory Powers Bill to Parliament. The Bill addressed the use and oversight of investigatory powers by NSLE agencies and reflected key aspects of the 198 recommendations of the three 2015 reports.[84] The draft Bill was published for prelegislative scrutiny and numerous aspects of the Bill were amended during its 2016 parliamentary passage. In essence the Bill outlined a new framework of powers and safeguards in relation to the interception of communications and

[78] *Data Retention and Investigatory Powers Act 2014* (UK) s 7, quoted in ibid 15 [1.1] (emphasis omitted).

[79] ISC, 'Press Release' (Press Release, 12 March 2015) 1, 3.

[80] *RUSI Report* (n 31) 1 [0.1].

[81] Ibid 1 [0.1]–[0.3].

[82] Ibid 1 [0.2].

[83] Ibid.

[84] Secretary of State for the Home Department (UK), *Draft Investigatory Powers Bill: Guide to Powers and Safeguards* (Cm 9152, 2015) 5.

the retention and accessing of communications data and associated activity such as equipment interference.[85]

The importance of public transparency was emphasised in all three 2015 UK reports. The ISC recognised the legitimate public expectation of openness and insisted that 'the Government must make every effort to ensure that as much information as possible is placed in the public domain' in order to 'improve public understanding and retain confidence in the work of the intelligence and security Agencies'.[86] RUSI described transparency as a means for enabling the public to engage in informed debate in order to reach agreement on 'a new, democratic licence to operate'[87] after the reinvigoration of the debate about privacy and security following the Snowden revelations.[88] Anderson discussed the importance placed on transparency by civil society organisations, describing submissions on the link between transparency and trust, the importance of clear and transparent authorising statutes in the context of the rule of law, the importance of public debate enabled by clarity and transparency in the operation of powers in practice, and the importance of publishing transparency reports with statistics on the operation of the regime in practice, including oversight mechanisms.[89] Even GCHQ has, according to Anderson, 'expressed a clear intention to be more transparent, wherever possible, about its capabilities and operations'.[90] Anderson himself linked transparency with the need to enable public debate and to engender trust.[91]

The various reports recognised, however, that transparency to the public cannot be absolute. The ISC referred to the need to strike a 'delicate balance',[92] RUSI referred to a 'perpetual dilemma',[93] while Anderson recognised a 'tension'.[94] Even producing the reports required navigation of this dual challenge, with the ISC discussing the use of its report to enhance transparency about how

[85] See ibid 5–9, 12–13, 16–17, 21–2.

[86] *ISC Report* (n 66) 8 [xix].

[87] *RUSI Report* (n 31) x, 102–3 [5.29].

[88] Ibid 29 [2.1].

[89] *Anderson Report* (n 47) 214–16 [12.6]–[12.16]; see also at 223–4 [12.33]–[12.35], 235 [12.76], 239 [12.88].

[90] Ibid 201 [10.42].

[91] Ibid 245–6 [13.1]–[13.3].

[92] *ISC Report* (n 66) 107 [279].

[93] *RUSI Report* (n 31) ix.

[94] *Anderson Report* (n 47) 192–3 [10.11].

data was collected and used by agencies, while also redacting the report to avoid a 'level of detail [that] would be damaging to national security'.[95]

While there are recognised tensions set out above, none of the reports suggested that one principle should dominate. All recognised that transparency could and should be enhanced. RUSI, for example, recognised that transparency and necessary secrecy are not incompatible, but rather that cultures of secrecy needed to be confined to operational activities where such secrecy is necessary and in the public interest; secrecy should not be allowed to extend to accountability and oversight mechanisms, ethical framework and policy documents, or 'as a means to avoid accountability or hide mistakes'.[96] This is consistent with Anderson's recommendation that *the operation* of covert powers remain secret while *intrusive capabilities and powers*, including their interpretation and justification, be made public.[97]

Recommendations of the various reports thus emphasised both transparency and secrecy. In all three 2015 reports, the need for transparency and the protected sphere of operational secrecy were not merely abstract, but fed into specific recommendations. For example, the ISC referred to the need for 'clarity and transparency' in justifying its recommendation for reform of the *Telecommunications Act*,[98] its recommendation that new legislation should 'clearly list', describe and justify 'each intrusive capability',[99] and its recommendation that the government publish 'information as to how these arrangements will work (for example, in codes of practice)'.[100] Transparency is captured in Anderson's fourth principle,[101] focusing on clarity in authorising statutes. It underlies a number of his recommendations and features more explicitly in recommendations 121–4.[102] Both transparency and secrecy were among RUSI's 'Ten Tests for the Intrusion of Privacy';[103] in particular, Test 8 requires that '[a]nything that does not need to be secret should be transparent to the public; not just comprehensible to dedicated specialists but clearly stated in ways that any interested citizen understands'.[104] This led to recommendation 2 which explicitly

[95] *ISC Report* (n 66) 11 [12].

[96] *RUSI Report* (n 31) 101 [5.20]–[5.21]; see also at 112 [5.61]–[5.62].

[97] *Anderson Report* (n 47) 8 [34].

[98] *ISC Report* (n 66) 118 [VV].

[99] Ibid 118 [YY].

[100] Ibid 120 [BBB].

[101] *Anderson Report* (n 47) 252–3 [13.31]–[13.34].

[102] Ibid 306 [121]–[124].

[103] *RUSI Report* (n 31) 104–5 [5.35].

[104] Ibid.

refers to the need for statutes to be 'written in plain and accessible language and include details of implementation and technical application of the legislation'.[105] The three 2015 reports therefore recognised the need for transparency as a default that should operate absent a need for secrecy in a specific context; all agreed that a culture of secrecy should not grow beyond the realm where it is strictly needed for operational effectiveness.

Increased transparency was thus one of the main objectives of the draft Investigatory Powers Bill. The government explained it as follows:

> [T]he Bill makes more explicit the powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies.[106]

The increased transparency was generally welcomed during the initial consultations on the draft Bill.[107] A notable exception was the ISC, which expressed disappointment that the draft Bill did not go far enough.[108] The ISC criticised a number of aspects of the draft Bill, including the lack of transparency regarding the concept of 'operational purpose'.[109] The government responded to this concern by referencing the provision of 'a list of draft operational purposes' to the ISC.[110]

While the Bill remained controversial, its passage was marked by a significant amount of scrutiny and debate.[111] The draft Investigatory Powers Bill, published on 4 November 2015, was for example examined by the ISC, the House of Commons Science and Technology Committee and a Joint Committee of both Houses.[112] Recommendations made by these committees were reflected in

[105] Ibid 107.

[106] Secretary of State for the Home Department (UK), *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny* (Cm 9219, 2016) 7 [9].

[107] See, eg, Pam Cowburn, 'First Take on the Investigatory Powers Bill', *Open Rights Group* (Blog Post, 5 November 2015) <www.openrightsgroup.org/blog/2015/investigatory-powers-bill>, archived at <https://perma.cc/NF2Y-4RK9>.

[108] ISC, *Report on the Draft Investigatory Powers Bill* (House of Commons Paper No 795, Session 2015–16) 1–2 [4]–[5] ('*Report on the Draft Investigatory Powers Bill*').

[109] Ibid 10 [J].

[110] Secretary of State for the Home Department (UK), *Investigatory Powers Bill* (106) 84.

[111] See David Anderson, *Report of the Bulk Powers Review* (Cm 9326, 2016) 9 [1.22]; Burkhard Schafer, 'Surveillance for the Masses: The Political and Legal Landscape of the UK Investigatory Powers Bill' (2016) 40 *Datenschutz und Datensicherheit* 592, 595.

[112] *Report on the Draft Investigatory Powers Bill* (n 108); House of Commons Science and Technology Committee, *Investigatory Powers Bill: Technology Issues* (House of Commons Paper

the Investigatory Powers Bill introduced on 1 March 2016. A House of Commons Public Bill Committee considered the Bill in 16 sittings.[113] Further committees that considered the Bill include the Joint Committee on Human Rights,[114] the House of Lords Select Committee on the Constitution,[115] and the House of Lords Delegated Powers and Regulatory Reform Committee.[116] Most of these committees took public written and oral public evidence running into thousands of pages.[117] In addition, and flowing from the debates and political questions regarding the utility of the bulk data powers, the operational case for the exercise of bulk powers was reviewed by the Independent Reviewer of Terrorism Legislation.[118] The review considered about 60 case studies provided by intelligence agencies, reviewed associated intelligence reports and documents, and questioned 85 intelligence officials, including on whether other methods could have achieved the same results. It found in its public report that there was a proven operational case for three of the bulk powers, and that there is a distinct (though not yet proven) operational case for bulk equipment interference.[119]

Increased transparency is visible in various elements of the *Investigatory Powers Act*. Importantly, powers to access data, especially bulk data, are clearer. The matters to be considered before a bulk interception warrant can be issued, the processes for issuing such a warrant, its reach and the controls that apply to it are, for example, detailed to a far larger extent than before.[120] While the fact

No 573, Session 2015–16); Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill* (House of Lords Paper No 93, House of Commons Paper No 651, Session 2015–16).

113 Joanna Dawson, *Investigatory Powers Bill: Committee Stage Report* (House of Commons Briefing Paper No 7578, 2 June 2016) 3.

114 Joint Committee on Human Rights, *Legislative Scrutiny: Investigatory Powers Bill* (House of Lords Paper No 6, House of Commons Paper No 104, Session 2016–17).

115 Select Committee on the Constitution, *Investigatory Powers Bill* (House of Lords Paper No 24, Session 2016–17).

116 Delegated Powers and Regulatory Reform Committee, *Children and Social Work Bill [HL]: Government Amendments, Investigatory Powers Bill, Bus Services Bill [HL]: Government Response, Children and Social Work Bill [HL]: Government Response* (House of Lords Paper No 21, Session 2016–17) 3–6 [10]–[28].

117 Anderson, *Report of the Bulk Powers Review* (n 111) 9 [1.22].

118 Ibid annex 2, 136 [1]–[5].

119 Ibid 1, 122–4 [9.12]–[9.15].

120 See *Investigatory Powers Act* (n 47). Previously there was little transparency concerning the warrants that enabled the intelligence services to collect bulk data about online and phone traffic: see, eg, *Telecommunications Act 1984* (UK) s 94. Even the fact that such warrants could be issued was not known. In a 2016 report the Interception of Communications Commissioner's Office revealed that 15 such warrants were in force: Burnton (n 67) 29 [8.33].

that a warrant has been issued will not be publicised, the key elements of the framework in terms of which a warrant can be issued are public. Greater publicity around these powers was helpful, for example, to inform the debate regarding the protection of key participants in public life.[121] As a result provisions were introduced to strengthen safeguards protecting journalistic material,[122] and in relation to equipment interference warrants where members of Parliament are concerned.[123] The Act importantly also provides more controls over decision-making; for example, by introducing a double-lock system requiring a Judicial Commissioner to review a decision of a Secretary of State to issue a bulk interception warrant.[124]

In addition, oversight has been strengthened by the creation of a new regulatory and supervisory body with appropriate powers, headed by the Investigatory Powers Commissioner, assisted by Judicial Commissioners.[125] The Act provides the Commissioners with extensive powers but also requires them not to act contrary to the public interest or prejudicially to national security, 'the prevention or detection of serious crime', or 'the economic well-being of the United Kingdom'.[126] A Commissioner must especially ensure that he or she does not

> a) jeopardise the success of an intelligence or security operation or a law enforcement operation,
>
> b) compromise the safety or security of those involved, or
>
> c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces.[127]

The balance between disclosing what can be disclosed and protecting what should be secret by necessity is also illustrated by the provisions regarding public reporting by the Investigatory Powers Commissioner. The Commissioner must prepare a detailed annual report for the Prime Minister.[128] The report must be published and submitted to Parliament.[129] The Prime Minister may,

121 See Anderson, *Report of the Bulk Powers Review* (n 111) 19 [1.60].

122 *Investigatory Powers Act* (n 47) s 154.

123 Ibid s 111.

124 Ibid ss 178–9.

125 Ibid s 229. See generally Lorna Woods, 'United Kingdom: The Investigatory Powers Act 2016' (2017) 3 *European Data Protection Law Review* 103.

126 *Investigatory Powers Act* (n 47) s 229; see especially at s 229(6).

127 Ibid ss 229(7)(a)–(c).

128 Ibid s 234.

129 Ibid s 234(6).

however, after consultation with the Commissioner and, where relevant, other functionaries, exclude from publication any part of such a report if the Prime Minister believes that publication of that part would be contrary to the public interest or prejudicial to

> a) national security,
>
> b) the prevention or detection of serious crime,
>
> c) the economic well-being of the United Kingdom, or
>
> d) the continued discharge of the functions of any public authority whose activities include activities that are subject tto review by the Investigatory Powers Commissioner.[130]

Where any part has been excluded from publication, the report before Parliament must be accompanied by a statement to that effect.[131]

The *Investigatory Powers Act* has also provided some support to the Investigatory Powers Commissioner to deal with the challenges posed by technology in terms of expertise (the second form of opacity in Burrell's taxonomy). It established a Technology Advisory Panel to be appointed by the Commissioner to advise the Commissioner and the Secretary of State about 'the impact of changing technology on the exercise of investigatory powers' overseen by the Commissioner, and 'the availability and development of techniques to use such powers while minimising interference with privacy'.[132] This would be in addition to increasing technical in-house resources for the oversight body promised by the government.[133]

The legislation remains controversial but it evidences attempts to improve transparency regarding powers and increased support for meaningful public debate. As one UK participant (P/P) stated: 'I just think the fact that they can write a 300-page Bill explaining what they do … means that there is so much about what can be revealed that doesn't imperil their effectiveness.' Nevertheless, the focus with the drafting of the *Investigatory Powers Act* in the UK was

[130] Ibid ss 234(7)(a)–(d).

[131] Ibid s 234(6)(b).

[132] Ibid ss 246(1), 247(1). See also Anderson, *Report of the Bulk Powers Review* (n 111) 124–8 [9.18]–[9.32] for the recommendation to establish the panel.

[133] Investigatory Powers Commission, 'Investigatory Powers Bill' (Fact Sheet).

primarily on transparency of powers, rather than algorithmic transparency in the NSLE context.[134]

IV Prospects for Greater Transparency in Australia

A *Prospects for Transparent Legal Powers and Open Debate*

In the case of Australia, the relative lack of clear transparency as to legal powers in relation to the collection, access and use of data for NSLE purposes seems more an accident of complex legal drafting, and patchwork solutions to agency needs, than a deliberate policy to obfuscate. In particular, as discussed above, research participants (including those in government) were generally in favour of greater transparency as to government powers.

The UK approach to reforming and clarifying its legal and regulatory regime provides a way forward for Australia, as well as confidence that these kinds of clarifications are ultimately a social good. While some may hesitate to bring public concerns out into the open, there is no other way forward for a democratic country seeking simultaneously to protect both the security and privacy of its citizens by ensuring that NSLE powers are used in publicly endorsed ways. It was therefore encouraging that the *2017 Independent Intelligence Review* into the Australian intelligence community recommended that a more transparent legal framework should be devised. They advised that a 'comprehensive review of the Acts governing [the] community be undertaken to ensure [that] agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians'.[135] This review, it was stated, should be aimed at drafting a legislative framework that is easily understood and accessible, resulting in greater transparency that would build public confidence in the community.[136]

To meet such an objective, the rules as to when agencies can collect data or access particular datasets need to be clear. In addition, there should be clarity about public accountability mechanisms, including oversight mechanisms, as these ensure that the system is deserving of public trust. These should not be confined to internal process documents and confidential memoranda of understanding between agencies. Apart from any other reason, maintaining secrecy

[134] More recently, there have been further initiatives to deepen the thinking around non-NSLE data governance in the UK, extending to algorithmic transparency: see, eg, *Royal Society Report* (n 57) 93–4, 98–9; British Academy for the Humanities and Social Sciences and The Royal Society, *Data Management and Use: Governance in the 21st Century* (Report, June 2017) 47–9, 55, 57.

[135] *2017 Independent Intelligence Review* (n 36) 92 [6.12].

[136] Ibid 92 [6.13].

as to what agencies are permitted to do is becoming increasingly difficult. As the Snowden leaks demonstrated, lack of assurance of complete cybersecurity means that NSLE agencies and policymakers will need to understand how to manage inevitable disclosures. In our view, this is best managed by ongoing public transparency, in clearly drafted legislation, as to the circumstances in which the public's data is collected, accessed and used.

Public engagement requires more than clear, transparent legal rules and regulation, it also requires some transparency about the public justification or 'operational case' for using data. Interviews revealed that from the Australian agency perspective, public engagement was specifically linked with the importance of the public better understanding *why* NSLE agencies need particular types of data, when privacy may not be appropriate, and how effective existing oversight regimes are. Of course, there is no guarantee that the public will take the same perspective on these issues as those working within the agencies. As one participant (T/T) acknowledged, '[i]t's going to be a very hard road to sell that message.' The use of the word 'sell' here, also used by another participant (O/O), who stated that '[y]ou need to sell why these things are needed', seems to treat the public as an audience rather than as active participants in a debate. The same tendency to treat the public communication as a one-way process can be seen in the comments of another research participant:

> Because I think a challenge would be to bring the community along, and they're going to have to believe that this is necessary, and they're going to have to trust that it's all going to be done with lots of transparency and lots of authenticity (P/P).

Other language used by some research participants similarly suggested that public opposition is something to be overcome, for example: 'The risk is public discomfort with change, it is hard to adapt' (T/O). Indeed, some research participants make assumptions about the public analogous to early advocates of public understanding of science, namely that there is a public deficit of knowledge that needs to be filled.[137] While there is a need to inform the public to bring them up to the level of knowledge because 'public perception of our requirements and our oversight and our access to data is far from the reality' (T/O), this cannot be sufficient. There needs to be a two-way discussion that goes beyond the assumption that government is right and only needs to win the hearts and minds of the people.

[137] The public deficit model was rejected in the Select Committee on Science and Technology Committee, *Science and Society* (House of Lords Paper No 38, Session 1999–2000) ch 2.

Strategies around public engagement and transparency going beyond mere public education were more prominent in the UK interviews. This arose in various forms, including: the need for government to be more open and transparent about benefits and risks (P/P); the need for government to be more open about justification for particular operational capabilities[138] and to engage with the public in an 'evidence-driven debate about the use of Big Data' (P/P); the importance of structured public engagement, including deliberative workshops held with the public over two days involving responses to scenarios and testing of a data ethics framework (P/P); and early engagement (by government and technology companies) with relevant NGOs concerned about particular ethical issues in order to facilitate mutually satisfactory problem-solving (P/P). Such engagements often gave government insights into the public's views that were not available elsewhere (P/P) and persuaded those otherwise concerned about privacy that particular powers (such as IP address-matching) were necessary (P/P). Public engagement can be an opportunity for mutual learning where 'proper' and 'open' conversations provide a 'safe space where the two sides can get to understand each other's views' and thus enable lateral thinking as to how to achieve both security and privacy (P/P).

Currently, in Australia, there is very little attempt to engage with the public around NSLE agency powers. As one participant (O/O) noted, this cannot be done by the agency analysts themselves but rather depends on official agency media engagement or politicians. Six Australian participants in the policy group discussed the possibility that existing conflicts in viewpoints about agency use of Big Data could be resolved through conversations, discussions or debates, either among specific stakeholders or more broadly. The nature and manner of the conversation was described differently by participants:

> [H]aving a decent and non-hysterical conversation with the community and particularly advocates about what is privacy (O-P/O).
>
> I actually think you should take a set of people from civil society — and I don't mean the soft pleasant ones — in Australia and lock them in a room with a set of intelligence agents and law enforcement and spend about two days role-playing a set of scenarios (P/P).
>
> [C]ollaboration in the development of these types of legislations and policies (P/P).
>
> Big and important debates, and they have to happen in an open environment (P/P).

[138] This was a position put by many civil liberties groups: *Anderson Report* (n 47) 215–16 [12.11]– [12.14].

> [Young people] should be involved in the creation of any policy in this area (P/P).

One research participant made the point that 'stakeholders' should not have privileged access to the debate because 'this is all equally everyone's concern' (P/P). Two research participants identified practical challenges in facilitating such a conversation, including time, media sensationalism and money. One pointed out that the end result of such a consultation would not necessarily be compromise, but rather the outcome of an argument (P/P).

Whatever form it takes, the public ought to be able to freely raise concerns about government powers to collect and access data for NSLE purposes. This requires greater clarity and transparency about what those powers are, how they are justified and what protections and oversight mechanisms exist. The UK demonstrates both that Australia can move much further in this direction and that, while operational secrecy is important, it can, but should not, unduly reduce transparency.

B *Prospects for Internal Algorithmic Transparency and Public Algorithmic Translucency*

In Part II(C), we explained why full public disclosure of the source code of algorithms is both undesirable and likely ineffective. However, it is important to maintain justified public trust in the way that data analytics are used to draw inferences about individuals that are employed in the course of agency decision-making. What we propose is public algorithmic 'translucency', involving important but limited information about the algorithms and full transparency to those with independent oversight roles over NSLE agencies combined with sufficient resourcing (including technical expertise). This goes beyond the reforms in the UK, although these have begun to deal with the question of technical expertise for oversight agencies. In addition, thought needs to be given by agencies to the types of algorithms deployed, a decision that we argue should be overseen by independent oversight agencies. Appropriate consideration may lead to limits being placed on the use of some complex, non-transparent algorithms that fall within Burrell's third category of opacity.

The idea of 'translucency' was mentioned in a Ditchley Foundation report,[139] by analogy to a partial view of what is going on behind frosted glass. It

[139] 'Intelligence, Security and Privacy: A Note by the Director', The *Ditchley Foundation* (Web Page, 14–16 May 2015) <www.ditchley.co.uk/conferences/past-programme/2010-2019/2015/intelligence>, archived at <https://perma.cc/5G96-2NHH>.

illustrates that often disclosure is not a question of all or nothing, but that it may be possible to enhance public confidence through some disclosures, while limiting access to material the disclosure of which would compromise operational effectiveness.[140]

There are ways of providing the public with some information about algorithms without disclosing the source code or underlying data. In fact, even the idea of disclosing 'source code' masks a range of levels of transparency depending on the coding language and the level of deliberate or inadvertent obfuscation.[141] Kroll et al challenge the 'dominant position in the legal literature' that transparency is the best means to demonstrate the 'fairness' of an algorithmic process.[142] They propose other technological tools that can be used 'to verify and demonstrate compliance with key standards of legal fairness for automated decisions without revealing key attributes of the decision or the process by which the decisions were reached'.[143] Their concerns with transparency include all three of Burrell's categories, namely operational secrecy and trade secrets, the inutility of disclosing source code given its lack of broader comprehensibility, and the emergent properties of machine learning algorithms. Instead, they suggest particular tests that can be conducted to determine compliance with particular standards of legal fairness, in particular procedural regularity (that the same procedure is applied to all) and non-discriminatory impacts. The tools they propose are said to be able to assess for procedural regularity while preserving the secrecy of the actual decision system.[144]

Kroll et al suggest that these techniques are not about transparency.[145] We disagree. What these tools do is to provide information with *limited* transparency, or what might be called translucency. For example, one of the proposed techniques, cryptographic commitments, simply specifies the timing of disclosure and/or the audience to whom information is disclosed, protecting disclosable information in the interim using cryptographic techniques. Another technique, zero knowledge proofs, can provide information about some aspects of a system while maintaining the secrecy of others, for example by demonstrating

[140] Ibid. On contexts in which public transparency is most useful, see generally Zarsky (n 48).

[141] L Jean Camp, 'Varieties of Software and Their Implications for Effective Democratic Government' in Christopher Hood and David Heald (eds), *Transparency: The Key to Better Governance?* (Oxford University Press, 2006) 183, 185–8.

[142] Joshua A Kroll et al, 'Accountable Algorithms' (2017) 165 *University of Pennsylvania Law Review* 633, 633–4.

[143] Ibid 634.

[144] Ibid.

[145] See especially ibid 657–60.

that changing particular characteristics does not affect the output without disclosing the actual algorithm. Machine learning techniques such as regularisation or the use of fair synthetic data, are only helpful in this regard if algorithms are required to use those specific techniques, which itself requires transparency about the algorithms being deployed. None of the proposed techniques avoids the need for *some* transparency. Thus, while we agree that accountability can be aided by transparency that is less than full public disclosure of source code and data,[146] it will still require a degree of transparency.

As Kroll et al explain, it is possible to disclose some information about algorithms that may be crucial for fairness and accountability without disclosing source code. This was also a point made by some Australian research participants. The goal should, according to one participant (P/P), be to make disclosure the default while not 'disclosing methods' that are 'the tools of the trade' and that need to be protected. Specific suggestions from research participants in both jurisdictions included 'the analytics that could be run in principle' (P/P), the fact that machine learning (for example) is being used (P/P), the extent to which the algorithms are 'being used in a discriminatory way' (P/P), information that gives 'an understanding of the potential for error — that is, false positives and false negatives' (P/P) and characteristics of algorithms such as that they 'meet this industry standard or whatever it might be' (O-P/O). Another suggestion was to make disclosures based on scenarios involving automated analysis, possibly with screenshots, that explain how data is used (P/P). There is also reference in the literature to explanations that focus on whether a particular factor is relevant or crucial to a decision, and why similar or different situations yield different or similar decisions, respectively.[147] These alternatives do not provide a full explanation of why an algorithm may reach a particular conclusion, but nevertheless assure the public that the algorithm is operating within particular parameters on crucial issues (such as procedural compliance and non-discrimination). They do so through translucency, or partial disclosure.

In some contexts, this kind of information or disclosure is actually more useful to the public than source code, as it does not require an ability to read code and can be used to understand elements of the behaviour of an algorithm.[148] The general public could perhaps be given limited access to the algo-

[146] Cf Citron (n 56) 1308–9.

[147] Finale Doshi-Velez and Mason Kortz, 'Accountability of AI under the Law: The Role of Explanation' (Working Paper, Berkman Klein Center Working Group on Explanation and the Law, 21 November 2017).

[148] This is noted in the *Royal Society Report* (n 57) 94.

rithm in operation for the purposes of testing particular features, such as differential impact on racial minorities. Technically, there are various tools that can be used to enable such limited disclosure about an algorithm. These include 'Quantitative Input Influence' measures that 'capture the degree of influence of inputs on outputs of … system[s]', preserve differential privacy and can be generated with 'black-box access' to a machine learning system.[149] Such limited access is an example of what we are calling algorithmic 'translucency'.

Another comparator is the European Union's *General Data Protection Regulation*.[150] This contains transparency requirements and restrictions on automated processing, albeit ones that have been criticised as limited and ineffective.[151] It is important to note that member states 'may restrict by way of a legislative measure the scope' and obligation of both rights in the context of national security, defence, public security and law enforcement, provided that 'such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard'.[152] There is also a broad carve out for the processing of personal data 'by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security',[153] being matters dealt with under a separate directive.[154] A provision for translucency, discussed here, may be an important component in ensuring that compliance with 'fundamental rights and freedoms' can be monitored by the public. However, our proposal operates quite differently to the Regulation, and

[149] Anupam Datta, Shayak Sen and Yair Zick, 'Algorithmic Transparency via Quantitative Input Influence' in Tania Cerquitelli, Daniele Quercia and Frank Pasquale (eds), *Transparent Data Mining for Big and Small Data* (Springer, 2017) 71, 73.

[150] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*General Data Protection Regulation*').

[151] Ibid arts 15, 22. For an example of critique, see Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking for' (2017) 16 *Duke Law and Technology Review* 18.

[152] *General Data Protection Regulation* (n 150) art 23(1). Note that the requirements in art 23(2) must be met by the legislative measure.

[153] Ibid art 2(2)(d).

[154] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA* [2016] OJ L 119/89.

is targeted at broad public transparency rather than provision of information to affected individuals.

Where the audience has security clearances, as in the case of independent oversight bodies, the degree of disclosure can and should be greater. As noted above, most research participants were comfortable with full transparency in this case. An oversight body should be in a position to satisfy itself that algorithms are functioning and being used in legally compliant and appropriate ways. They should also have access to information on how the algorithm was used, who or what it identified as threats and so forth, and so can statistically test whether the algorithm as used in practice operates in ways that unfairly discriminate. They also have sufficient access to systems to conduct audit studies,[155] including where relevant in relation to systems operated by networks of agencies.[156] While some of this can be achieved through similar 'translucency' devices, we believe such agencies should have, in principle, access to both source code and datasets. The extent to which they can make use of that to maintain effective oversight is, of course, a question of expertise. Ideally, oversight bodies should be able to secure sufficient technical expertise in-house.

While one research participant, quoted above in Part II(C), suggested that oversight agencies should rely on the expertise within operational agencies, we are concerned that, without technical expertise, oversight agencies may not be aware of the assumptions that underlie the use of data analytics. Even to understand what evaluations are important and how they ought to be conducted requires technical expertise. If oversight agencies are solely reliant on the operational agencies for this expertise, the potential for issues to be missed is greater. As a result, there is a risk that the community will lose trust in the agencies, particularly if there are differential impacts on marginalised communities. If the public cannot fully verify the algorithms themselves, there should at least be an independent evaluator with the access and expertise to do so. The UK proposal to establish the Technology Advisory Panel and provide additional resources for technical oversight is a positive step in this regard.[157]

[155] See Christian Sandvig et al, 'Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms' (Conference Paper, Data and Discrimination: Converting Critical Concerns into Productive Inquiry, 22 May 2014) 5–18.

[156] On the need for network accountability in the context of US 'fusion centres', see Danielle Keats Citron and Frank Pasquale, 'Network Accountability for the Domestic Intelligence Apparatus' (2011) 62 *Hastings Law Journal* 1441.

[157] The *2017 Independent Intelligence Review* recommended the establishment of a National Intelligence Community Science and Technology Advisory Board. This Board however would seem to be focused on the development of joint capabilities and not necessarily on supporting oversight functions: *2017 Independent Intelligence Review* (n 36) 80–1 [5.25].

The final element in our proposal is that careful thought should be given to the types of algorithms and processes that agencies employ. There are choices here. Some software is commercial-in-confidence which compounds the problems of state or operational secrecy. Some machine learning processes are opaque as to their inner logic while others preserve their provenance, enabling an analyst to discover the data on which particular inferences are based.[158] There are costs and benefits here too — a complex machine learning algorithm with emergent, unpredictable properties that is subject to commercial-in-confidence provisions may be the best available means to make particular predictions, interrogate particular data or preserve operational secrecy. It is thus crucial that those making these choices be conscious of the various factors involved, and that their choices be justified both internally and to independent oversight bodies with access to both sufficient expertise and resources for evaluation. In our view, algorithms with complex, emergent, unpredictable properties should not be used to draw inferences against individuals as the basis for making decisions that will have a direct negative impact on those individuals (for example, in preventative detention or bail).[159]

V Conclusion

There is a variety of lessons that can be learned about how to enhance transparency in the collection, access and use of data for NSLE purposes in Australia by listening to operational, technical and policy stakeholders, understanding the current legal framework, learning from comparable jurisdictions such as the UK and drawing on the growing literature about algorithmic transparency and accountability. Transparency is an important element in the use by NSLE agencies of powers that provide them with access to personal information and tools that enable the analysis of that information. Public trust in the system should be supported through transparency of intrusive powers as well as control measures and accountability and oversight mechanisms, and confining secrecy to those aspects of operational activities where secrecy is necessary and in the public interest. Powers, control measures and accountability and oversight mechanisms need to be clearly set out in publicly available laws and regulations, rather than hidden in internal manuals, memoranda of understanding or letters

[158] For example, the Defense Advanced Research Projects Agency ('DARPA') has a program of work on explainable artificial intelligence: David Gunning, 'Explainable Artificial Intelligence (XAI)', *DARPA* (Web Page) <www.darpa.mil/program/explainable-artificial-intelligence>, archived at <https://perma.cc/M96Z-JJXX>.

[159] See *Royal Society Report* (n 57) 93–4.

of agreement. In creating and reviewing these rules, government should provide opportunities for public debate and engagement around agency powers, particularly in relation to 'bulk' access to personal data, that incorporate a discussion about the opportunities presented by government use of data and analytics and an airing of concerns about risks.

Algorithmic transparency to agency management and oversight bodies combined with algorithmic translucency to the general public is significant in facilitating accountability in decision-making and should be pursued despite its practical difficulties. Appropriate expertise should be available to oversight agencies to enable them to review the ways in which data and algorithms are used in NSLE agencies, whether internally or through an independent external body. Algorithms that are inherently opaque (so that the proposed internal transparency and external translucency is not possible), whether due to complexity or commercial terms, should not be used by government where inferences drawn lead to negative impacts on individuals. Thus opacity should be an important factor in selecting software products for particular uses.