Comprehensive Review

Legal Framework of the National Intelligence Community

Public Submission of Dr Philip Glover, School of Law, Curtin University, Perth, Western Australia. [redacted]

Introduction and Statement of Credentials

I am a Lecturer in Law at Curtin University and my research interests encompass data/communications access/investigation and prejudice-related crime. I obtained my doctorate in the UK (University of Aberdeen). My 2015 doctoral thesis examined the then-existing UK legal framework regulating communications-related investigatory powers (RIPA 2000 in particular) and argued for a single statute regulating the acquisition of communications-related data (content and metadata) in a single statute.[1] Fortuitously, my research coincided with the post-Snowden UK parliamentary and independent reviews of RIPA 2000 (to which Australia's TIA 1979 has many similarities) and the broader communications investigation legal framework.[2] My research findings partially aligned with those of Lord Anderson's Investigatory Powers Reviews[3] and those of the UKPISC, to whom I provided oral and written submissions.[4] I have since published my doctoral thesis-based monograph as 'Protecting National Security: A History of British Communications Investigation Regulation' and my interest in this area of public law remains since achieving permanent residency in Australia. Chapter 2 of that book examines some of the conceptual issues raised herein.[5] I attended the public consultation chaired by Dennis Richardson at ANU in 2019 and my written submission to the Comprehensive Review was cited therein. Please cross-refer if you feel the need. This submission offers some general comment before addressing the Discussion Paper (DP) questions I feel qualified to answer.

[1] Philip Glover, 'Reconceptualise Investigatory Powers Again? An Argument for a Comprehensive Single Statute Regulating the Acquisition of Expression–Related Data for Investigative Purposes by UK Public Authorities' (PhD Thesis, University of Aberdeen 2015)
< https://abdn.pure.elsevier.com/en/publications/reconceptualise-investigatory-powers-again-an-argument-for-a-comp> .As the theoretical boundary between 'communication' and 'expression' remains blurred, the term 'communications-related data (CRD)' (explained in depth further herein) is preferred

[2] Principally, but not limited to, the UK Parliamentary Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (HC 2014-15, 1075-I) (UKPISC Privacy & Security Report); Anderson D, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (Williams Lea Group, June 2015) (Anderson Review) and the Royal United Services Institute (RUSI), *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (Royal United Services Institute for Defence and Security Studies, 2015) (RUSI Review).

[3] Including the Bulk Powers Review

[4] 20150312-P+S-017-Glover.pdf available at <http://isc.independent.gov.uk/public-evidence>

[5] Phil Glover, *Protecting National Security: A History of Communications Investigation Regulation* (Routledge International, 2021).

GENERAL COMMENT

Nomenclature

'Electronic Surveillance Act' does not describe the statutory purpose(s) sufficiently accurately. Many of the powers under review are not covert 'surveillance' powers. What is sought is a statute that enables certain Commonwealth Government and State government agencies with investigative functions to *access data* (whether at rest or in transit)[6] for particular investigative or national security purposes. Such data may itself be communicable, form part of a communication, or not. Given that data (whether or not *communicable*) constitutes the core raw material, consideration should be given to notifying the electorate that the Commonwealth is enacting a Data Investigation Act (DIA). Definitions, including that for 'communication' should be constructed around the reality that data is that core material.

Definitions

The nature of the data and datasets will require categorisation. This will not be easy. It can be categories according to its perceived intrusiveness to personal autonomy/privacy. It can be categorised according to its likely intelligence value. But it should not be impossible for combined expertise to compile a taxonomy of data categories that allow an appropriately properly constituted Data Investigation Oversight Commission, with responsibility for authorisation and ex post facto oversight, to harmonise the thresholds for authorising national security and serious crime-related warrants.

Question Responses

1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day? Insufficiently.

a) **If so, which aspects are working well?** There appears no difficulty with the current scope and construction of the existing criminal offences.

b) **If not, which aspects are not working well and how could the new prohibition and/ or offences be crafted to ensure that information and data is adequately protected?**

'Data', whether at rest or in transit, only becomes 'information' when rendered into intelligible form, whether to a human actor or AI overseen by human actors.[7] Once examinable data becomes capable of revealing anything tending to identify an individual or anything about their lived life, then information privacy protection considerations arise.

Given that information privacy is a global concept, it follows that information privacy considerations should be harmonised to the greatest possible extent across jurisdictions, particularly those with similar democratic principles (e.g. the EU and UK) or in a Five

[6] See for example, Joseph MacMillan, *InfoSec Strategies and Best Practices: Gain Proficiency in Information Security Using Expert-Level Strategies and Best Practices* (Packt Publishing, 2021) 56

[7] See my previous submission to the Richardson R

Country/FVEY relationship. At this embryonic stage of the statutory development process, suffice it to say that the current 'gold standard' in the protection of data is provided in jurisdictions adhering to the European Convention on Human Rights (ECHR). Any new AU statute should be drafted around similar principles. This involves critically examining the *nature* of the data to which access is sought, the *purpose(s)* for which such data requires investigation, the *necessity* of access, and the *proportionality* of (i) the investigative technique(s) to be deployed, and (ii) where accessed data is appropriated, the use(s) (including disclosure to other stakeholders) to which data will be put. If information privacy is to given adequate respect against the rightful protection of national security and prevention of serious crime, then a model such as the UK's Investigatory Powers Act 2016 can be instructive. It is no longer the nature of the investigating agency, or perceived degree of intrusion, that should dictate what is to be sought, but the utility of the data to be accessed balanced against the ramifications for privacy.

2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives of societal benefit, e.g. cyber security of networks, online safety, scam protection/reduction?

They could be clearer. Australia's current data protection framework is insufficiently robust. It is also insufficiently clear. There is insufficient transparency about how and when government agencies with data investigation functions can access data.

3. Are there any additional agencies you consider should have powers to access particular information and data to perform their functions? If so, which agencies, and why?

At the risk of embarrassing myself by having missed something blindingly obvious, I am at a loss as to why the ASD (and even perhaps ASIS) are not mentioned in these consultations and seem to fall outwith the scope of the proposed DIA. The nature of the internet has rendered the current definition of 'foreign communication' virtually meaningless, and it appears improbable that electronic data, either constituting communications or forming part thereof, are not accessed by ASD. Given that these are sent from AU, often by Australians, surely the same information privacy considerations should apply to data in transit from AU?

If serious about transparent secrecy, as Rachel Noble has described it, all your data investigation and data-surveillance powers (e.g. foreign communications screening) need to be avowed.

4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

Any Commonwealth/State entity with data investigation functions should be included. Where the data sought is likely to identify person(s), then a uniform standard of privacy protection principles should apply, to be balanced against the necessity and proportionality of the investigative *purpose*(s).

PART 2: WHAT INFORMATION CAN BE ACCESSED?

5. Are there other kinds of information that should be captured by the new definition of 'communication'?

There is an inherent risk of circularity in defining 'data', 'signals', 'information' and 'communications' etc. Whilst data in transit can accurately be described as forming a communication or part thereof, data at rest may not always be 'communicable' or intended for communication. In line with my comment under 'nomenclature' previously, it might be technically easier to define data, and then a definitional 'hierarchy of data' (according to its likely privacy sensitivity). Should this not be approved, then the comprehensive definition of 'communication' in the UK's IPA 2016 is useful and instructive.

6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?

'Data' (at rest and in transit) is the core raw material.

7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?

Through acknowledging that data is more than a communicable construct. The UK IPA 2016 recognises (within its definition of communication) that 'things' can communicate. If that conceptual view is inverted, then any new AU Data Investigation Act can acknowledge that data (whether or not intended to ever be communicated) and wherever located, can be accessible for investigation.

8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information? Is there a quantity at which non-content information becomes content information and what kinds of information would this apply to?

The perils of defining content (e.g. by assumptions on the discernibility of a 'meaning') have been worked through comprehensively by the UK internet lawyer Graham Smith (See Cyberleagle blog). This is why my personal preference is for categories of data (I'm not pretending that categories of data are easy to create or arrange into a hierarchy), but if investigative entities are to be truly honest about respect for a right to have data privacy only infringed on a proportionate basis, then the law needs to recognise that infringements are case-specific, and related to the type of data sought, and the uses to which data will be put.

9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions which achieve the desired outcome?

My previous response refers. See also Philip Glover, Protecting National Security: A History of Communications Investigation Regulation (Routledge, 2021) Chapter 2, particularly at 38-40 examines this very question.

10. Are there benefits to distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?

Very much so. See previous responses. In my view 'content' is now something of a red herring. On one view, as Chapter 2 of my book notes, state access to content (e.g. a conversation) is highly intrusive and potentially very embarrassing, but a truly empathetic but effective investigatory powers statute would recognise that it is the intelligence product obtained through access, and the degree of privacy infringement brought about in creating or disclosing that product, that should dictate the authorisation mechanism, the oversight mechanism etc.

11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?

I don't think so, but remain open to persuasion by the experts. Data is data, whether stored or in transit. It is the potential intelligence product, and potential private information about the data subject(s) that is important.

12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?

Subject to what is stated later herein, whilst the degree of potential intrusion to a target's privacy, or the nature/amount of sensitive information revealed about them via investigation is important, the purpose of the investigation, (e.g. to produce info vital to protecting natsec) is of greater importance. These matters need to be assessed prior to investigative access, and the assessment should include input from independent expertise familiar with principles of proportionality

13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?

Any data communications/storage service should be included.

14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

The question is unclear. There needs to be definitions for 'data', 'information' (e.g. data in a form comprehensible to a data analyst (whether human or artificial) 'personal data'; 'sensitive personal data'; 'legally privileged data'; journalistic source data; communication. There needs to be clear definitions for each type of data potentially accessible by investigators. This needs a lot more work!

Part 3: How can information be accessed?

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?

If the focus is redirected to the likely *or intended product* of the data access, and *the purpose* (e.g. natsec) for which access to the data is sought, then authorisations could be harmonised on that basis. Whilst the UK's double lock system no win operation under the IPA 2016 is a step forward, AU could improve upon it. AU should establish a wholly independent Data Investigation Oversight Commission combining judicial expertise from, e.g. the AAT, to assess applications to investigate those categories of data likely or intended to be sought by applicants. The nature of the applicant should not determine the authorisation mechanism. Ministers tend to defer to the intelligence agencies and ex post facto oversight of Ministerial authorisation is too late for privacy concerns. The UK IPCO provides an embryonic model allowing for truly independent judicial scrutiny of Ministerial needs for the most serious cases and can also bring in the IGIS and even a tribunal for complaints. Technical advisors could also be considered to assist the judicial assessors.

Obviously a clearly defined data hierarchy needs to be established so that simple requests for, say, location data are authorised more locally. For true proportionality however, independent judicial scrutiny should be considered even for these.

16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?

See previous. Data as raw material should be categorised (in a manner not unlike CSEAM) according to the likelihood of private information compromiser balanced against investigative purpose. Not easy, but doable.

Part 4: When will information be accessed?

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?

These categories should be replaced by the data categories suggested. Whether the data is at rest or in transit is immaterial compared to the product of investigation**.**

18. Are there any other changes that should be made to the framework for accessing this type of data?

Strongly consider a Data Investigation Oversight Commission

19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?

20. What are your views on the proposed framework requiring warrants and authorisations to be targeted at a person in the first instance (with exceptions for objects and premises where required)?

Given the levels of collateral intrusion inevitable in data investigation/analytics, it seems more sensible to avoid targeting person(s) in the first instance, but to outline a clear investigative *purpose* and an outline of the likelihood of privacy intrusions to person.

21. **Is the proposed additional warrant threshold for third parties appropriate**? As **above**

22. Is the proposed additional threshold for group warrants appropriate? As above

23. **What are your views on the above proposed approach? And are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?**

There should be a single issuing authority for data appropriately categorised

24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?

Only for data in the lower categories once finalised

25. **What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?**

Disclosure should be purpose-based and on a need to know basis

26. When should agencies be required to destroy information obtained under a warrant?

When a review (after say, one year and undertaken by the IGIS wing of a new IPCO based Data Investigation Oversight mechanism) determines the relevant material no longer has intelligence/evidence utility.

27. What are your thoughts on the proposed approach to emergency authorisations

A Data Investigation Oversight Commission could oversee these

28. Are there any additional safeguards that should be considered in the new framework?

No.

29. Is there a need for statutory protections for legally privileged information (and possibly other sensitive information, such as health information)?

Absolutely. Again, once a cogent data classification basis has been established, a properly constructed oversight commission can assess applications for data access likely to discover or reveal these extra-sensitive categories

30. What are the expectations of the public and industry in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?

No comment

31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?

Bring the role within the ambit of a Data Investigation Oversight Commission

32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?

No comment

33. Are there any additional reporting or record-keeping requirements should agencies have to improve transparency, accountability and oversight?

There should be no closed drawers when oversight bodies come searching

Part 6: Working together: Industry and Government

34. How workable is the current framework for providers, including the ability to comply with Government requests?

No comment

35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?

No comment

36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way

No comment