WHO OWNS INFORMATION? LAW ENFORCEMENT INFORMATION SHARING AS A CASE STUDY IN CONCEPTUAL CONFUSION

LYRIA BENNETT MOSES*

This article addresses the real impacts of conceptual confusion surrounding statutory language linking entities and information for purposes such as privacy, freedom of information, archiving, policing and evidence laws. The idea of ownership of information (which is assumed in the statutory allocation of powers of control and responsibilities) is captured in a confusing miscellany of terminology that differs across jurisdictions and contexts. It uses the example of information sharing for law enforcement purposes as a case study to highlight the practical challenges inherent in the diverse and vague statutory language linking entities and information. It then proposes a new taxonomy for attributing responsibilities and powers with respect to information that is consistent with the ephemeral nature of the subject matter.

I INTRODUCTION

Just as the private sector proclaims that data is the new oil,[1] the Australian Government has described information it holds as a 'strategic national resource'.[2] Both government and businesses are increasingly conscious that analysing data promises benefits, seeing its potential for profit-making or for 'growing the economy, improving service delivery and transforming policy outcomes'.[3] The benefits are even more pointed in the context of law enforcement, where treating information as a 'national asset'[4] is seen to have a potential impact on the ability of agencies to prevent and investigate crime.

* Director, Allens Hub for Technology Law and Innovation and Professor, UNSW Law. The author would like to thank Sarah Logan for conducting interviews, Leah Grolman for her thorough research assistance, the anonymous reviewers for their thoughtful advice, and the *Journal* for editorial care. She also acknowledges funding from the Data to Decisions Cooperative Research Centre, and the support of colleagues in the Law and Policy stream, and the access provided by our government partner, the Australian Criminal Intelligence Commission.

1 See, eg, 'The World's Most Valuable Resource Is No Longer Oil, but Data', *The Economist* (online, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

2 'Australian Government Public Data Policy Statement', *Department of the Prime Minister and Cabinet*, (Policy Statement, 7 December 2015) 1 <https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf>.

3 Ibid.

4 See, eg, Australian Criminal Intelligence Commission, *Australian Criminal Intelligence Management Strategy 2017–20* (Strategy, 2017) 1 <https://www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2017-20.pdf>.

While information systems experts may argue that there are distinctions between data and information (so that information is data in context, or data plus meaning, or processed data), for current purposes they can be treated as synonymous. Albeit in a different context, the majority of the High Court adopted the ordinary meaning of the term 'information' as 'without necessary relation to a recipient: that which inheres in or is represented by a particular arrangement, sequence, or set, that may be stored in, transferred by, and responded to by inanimate things'.[5] While information can be stored in a physical medium such as paper, a computer disk or server, or even DNA,[6] information itself is ephemeral.

It is the ephemeral nature of information that makes it difficult to understand relationships that entities have with it. In the case of physical assets such as oil, property law allocates rights of control and responsibilities for harm. Even though property language (including the verb 'to possess') is often used in statutes to allocate particular responsibilities with respect to information and to identify specific entities as having powers to make certain decisions with respect to it, information is not property under the general law. Unlike the situation for oil, where the single legal category of property is all that is required to identify an 'owner' with control of and responsibility for the asset, statutes that link entities to information for the purposes of protecting individual privacy, guarding state secrets, ensuring proper archiving, facilitating access to government information, and mandating good data governance practices use a wide variety of terms and concepts. While there are important distinctions to be made among different kinds of relationships an entity might have with particular information, the diversity of terms used goes beyond what is necessary and some terms, such as those that treat information as analogous to a physical chattel, are confusing.

In particular, current statutory terminology is sometimes difficult to interpret in the context of new data practices. Off-site storage and processing of information, often referred to as cloud computing, stretch the interpretation of existing laws, forcing detailed analysis of obscure and outdated differences in terminology and definitions. Cloud computing allows information to be stored across multiple servers and jurisdictions, with access and control split among multiple entities, some of which may create derived information products from the raw data to which they have access. A cloud computing provider, with servers in multiple jurisdictions and data stored in different locations,[7] may host information provided by multiple entities (in different jurisdictions) and provide access to that information to multiple entities (in different jurisdictions). In the context of government, such information sharing may be based on intergovernmental agreements, memoranda of understanding or letters of agreement among the relevant agencies. There may be additional parties – entities accessing the information to provide data analytic services, providing data platform services that facilitate access to stored information, or editing stored information. One proposal being piloted while this research was conducted is the National Criminal Intelligence System ('NCIS'), a data-sharing platform for federal and state law enforcement information. The intention was for the NCIS to become a platform to which access was controlled,

5 *D'Arcy v Myriad Genetics Inc* (2015) 258 CLR 334, 371 [89] (French CJ, Kiefel, Bell and Keane JJ), quoting *Shorter Oxford English Dictionary* (5th ed, 2002) 'information' (def 3c).

6 Ibid.

7 See Organisation for Economic Co-operation and Development, 'Cloud Computing: The Concept, Impacts and the Role of Government Policy' (OECD Digital Economy Papers No 240, OECD, 19 August 2014) 19–20 <http://dx.doi.org/10.1787/5jxzf4lcc7f5-en>.

and automated protocols for information sharing implemented, based on attributes such as security clearance, agency, rank and so forth. As the variety of information storage systems increases, it becomes more difficult to identify the entity which 'holds', 'possesses' or has 'custody' of information. The relationship between entities and information has always had the *potential* to be many-to-one, but new technologies make this increasingly common.

These interpretative challenges are not purely theoretical. This article uses the example of information sharing for law enforcement purposes as a case study to highlight the practical challenges inherent in the diverse and vague statutory language linking entities and information. The case study was chosen because of its importance. The need to improve information and intelligence sharing in law enforcement has been mentioned in numerous reports and strategies over many years, including the Parliamentary Joint Committee on the Australian Crime Commission (2007, 2009),[8] the Clarke Inquiry (2008),[9] the *Street Review* (2008),[10] the *Smith Review* (2008),[11] the *Organised Crime Strategic Framework* (2009),[12] the *National Security Science and Innovation Strategy* (2009),[13] the *Beale Repo*rt (2009),[14] the *National Security Information Environment Roadmap: 2020 Vision* (2010),[15] the *Strong and Secure Report* (2013),[16] the Parliamentary Joint Committee on Law Enforcement (2013),[17] the *Review of Australia's Counter-Terrorism Machinery* (2015),[18] the *Joint Commonwealth-New South Wales Review* into the Martin Place Siege (2015),[19] the *Inquest into the Deaths Arising from the Lindt Café Siege* (2017),[20] and the *National*

8 Parliamentary Joint Committee on the Australian Crime Commission, Parliament of Australia, *Inquiry into the Future Impact of Serious and Organised Crime on Australian Society* (Report, September 2007) ch 8; Parliamentary Joint Committee on the Australian Crime Commission, Parliament of Australia, *Inquiry into the Legislative Arrangements to Outlaw Serious and Organised Crime Groups* (Report, August 2009) 130 [6.5], 141–9 [6.48]–[6.77].

9 MJ Clarke, *Report of the Inquiry into the Case of Dr Mohamed Haneef* (Report, November 2008) xii (Recommendation 9).

10 Sir Laurence Street, Martin Brady and Ken Moroney, *The Street Review: A Review of Interoperability between the AFP and Its National Security Partners* (Report, 14 March 2008) 12–13 (Recommendation 6) (concerning counter terrorism information sharing between AFP and ASIO) ('*Street Review*').

11 Ric Smith, *Report of the Review of Homeland and Border Security – Summary and Conclusions* (Report, 4 December 2008) 3 ('*Smith Review*').

12 Australian Government, *Commonwealth Organised Crime Strategic Framework: Overview* (Framework, 2009) 12, 15–16 capabilities 1 and 5 ('*Organised Crime Strategic Framework*').

13 Department of the Prime Minister and Cabinet, *National Security Science and Innovation Strategy* (Strategy, 2009) objective G.

14 Roger Beale, *New Realities: National Policing in the 21st Century* (Report, 30 June 2009) 19–20 recommendations 3.3, 3.5 ('*Beale Report*').

15 Department of the Prime Minister and Cabinet, *National Security Information Environment Roadmap: 2020 Vision* (Roadmap, 2010) ('*Roadmap*').

16 Department of the Prime Minister and Cabinet, *Strong and Secure: A Strategy for Australia's National Security* (Strategy, 2013) 43 ('*Strong and Secure Report*').

17 Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into the Gathering and Use of Criminal Intelligence* (Report, 15 May 2013).

18 Department of the Prime Minister and Cabinet, *Review of Australia's Counter-Terrorism Machinery* (Review, January 2015) 19–20.

19 Department of the Prime Minister and Cabinet, *Martin Place Siege: Joint Commonwealth – New South Wales Review* (Review, January 2015) 54, 58 (Recommendation 12).

20 State Coroner of New South Wales, *Inquest into the Deaths Arising from the Lindt Café Siege: Findings and Recommendations* (Report, May 2017) 13 [28], 21 [95], 39 [245]–[248], 392 [109] (Recommendation 39), 405 [135] (Recommendation 42).

Organised Crime Response Plan (2015–2018).[21] Relying on qualitative empirical data, this article argues that, while government leaders and authors of official reviews and policy documents bemoan cultures that resist greater information sharing in the context of law enforcement and the broader public service, public servants and law enforcement officials sometimes struggle to understand their obligations under confusing and often punitive laws. In other words, the barriers to greater information sharing in this field are at least partly attributable to legal complexity and, in particular, the failure of legislation to articulate clearly and consistently the relationship between information and particular entities.

This article thus proposes a new taxonomy for attributing responsibilities and powers with respect to information that is consistent with the ephemeral nature of the subject matter. There are important distinctions to be drawn among *relationships* between entities and information, in particular whether that entity has mere access to information, whether it has processed particular information, whether it has practical control over particular information, and whether it has possession of the medium on which information is stored. In allocating specific powers and responsibilities over information, these distinctions ought to be recognised. In particular, this article proposes that the wide diversity of terms used currently in legislation be replaced with a shorter list, such as 'has access to', 'process', 'control' and 'possession' (in relation to the physical medium on which information is stored) or synonyms of these. There is no need for new language identifying an individual to which personal information pertains.

While legal clarity around relationships between entities and information is not sufficient to ensure that information is shared efficiently and appropriately, it is a necessary precondition. The 'national asset' vision, if interpreted as implying that information ought to be untethered, ignores the need for particular actions to be taken by specific entities to ensure proper information governance. Efficient information sharing requires the use of cloud computing and data platforms that give rise to ambiguities in relation to control and responsibility. Appropriate information sharing requires contextualised decision-making by appropriately authorised officers. Other functions such as auditing, archiving and mandated disclosures require individuals with the responsibility to ensure that relevant legislation is complied with. The positive side of a 'national asset' vision, that information is shared efficiently and appropriately across agencies for national benefit, thus requires clear allocation of powers and responsibilities.

This article reports on research employing a range of methodologies, described in Part II, to articulate the problem and propose a solution. Part III draws on interviews with staff in relevant agencies to explore the diversity of current understandings of 'ownership' of information. While 'ownership' is too contested a term in this space to be helpful, the allocation of powers and responsibilities with respect to information remains central. Part IV turns to statutory allocation of such powers and responsibilities, highlighting the diversity of terminology to convey a more confined range of potential relationships between entities and information. Part V returns to interview data to explain how statutory confusion manifests in situations where the link between entities and information is complicated by modern data practices. It explains why linking data to specific entities in order to allocate powers and responsibilities is not in conflict with,

21 Australian Government, *National Organised Crime Response Plan 2015–18* (Plan, 2015) <https://www.homeaffairs.gov.au/criminal-justice/files/national-organised-crime-response-plan-2015-18-accessible.pdf>.

and may in fact support, appropriate information sharing envisaged by policy-makers who view information as a 'national asset'. Part VI outlines law reform options, explaining why an improved taxonomy for describing potential relationships with information is needed in addition to more targeted reforms currently being proposed. Part VII concludes.

II METHODOLOGY

This article seeks to draw links between practical issues in information sharing in the specific context of law enforcement and a broader legal framework that complicates the linking of entities to information. It relies on interviews for the former and a survey of legislation for the latter.

A Interviews

As part of a broader research project seeking to understand obstacles to information sharing for law enforcement purposes in Australia,[22] 31 semi-structured interviews were conducted with research participants who had relevant knowledge of and expertise in the usage, classification, sharing and management of data within the context of law enforcement information sharing.[23] Interviewees included both senior and operational staff currently or formerly associated with the Australian Criminal Intelligence Commission ('ACIC') and select partner agencies, in particular New South Wales Police, Victoria Police, the Australian Federal Police, the Department of Immigration and Border Protection, and the Australian Tax Office. Twenty-three interviews were conducted in person, and eight by phone, between 17 April and 26 May 2017. Three were transcribed live, while the remainder were recorded for subsequent transcription. Recruitment of interviewees was facilitated by the ACIC, but invitations were sent directly by researchers. The sample of 31 research participants was not randomly selected to be representative of the population of law enforcement staff who had knowledge of, and expertise in, data usage and sharing and thus observations in this section do not necessarily represent the full range of views in this population. Research participants were identified by a code consisting of a role identifier (operational O, operational requiring specific approval for release of quotes OC, public service P, public service requiring specific approval for release of quotes PC, and ACIC which requires specific approval for release of quotes AC). OC, PC and AC quotes used in this article were approved for public release.

Research participants were asked about their understanding of 'ownership' of information, in particular about the way in which this notion was conceived and the way in which 'owners' could be identified. We started with the idea of ownership for several reasons. The notion that agencies 'own' data is referred to in important government documents such as the *Information Security Manual*.[24] The importance of agencies maintaining 'ownership' of information has been raised in relation to the merger of CrimTrac and the Australian Crime Commission that formed the basis for the

22 Reports setting out the findings of the broader research project are available at 'Law & Policy', *Data to Decisions CRC – Legacy* (Web Page) <https://www.d2dcrc.com.au/law-policy>.

23 This research was approved by the UNSW Human Research Ethics Advisory Panel on 4 January 2017 (Reference number: HC16972).

24 Department of Defence, *Australian Government Information Security Manual: Controls* (Manual, 2016) 19–20, 33 ('*Information Security Manual*').

development of the NCIS system.[25] The idea of information 'ownership' by agencies or within jurisdictions is sometimes cast as a barrier to greater information sharing or to the 'national asset' idea.[26] It was therefore a useful starting point from which to explore the ways in which and purposes for which entities are linked to information. However, while the interviews began with the idea of 'ownership', they diverged into questions concerning making decisions about information, taking responsibility for statutory obligations relating to information, as well as control and responsibility for information held in the cloud or on a data sharing platform such as NCIS.

Not only was interview data useful for highlighting the roles that the concept of ownership can play in allocating powers and responsibilities (Part III), it also illustrated some of the practical challenges that result from conceptual confusion in this area (Part V).

B Survey of Legislation

There are a number of statutes that draw links between information and Australian law enforcement entities for the purposes of allocating powers or responsibilities. My research assistant, Leah Grolman, began with a range of terms that are commonly used to link information and entities, namely possess*, property, acquir*, obtain, responsible for, control, custody, hold*, and access. Using these, together with 'data or information or record* or document*' in the search function within Austlii, a range of statutes were identified at the Commonwealth level and in each of Australia's six states and two mainland territories. These deal with a diverse range of subject matters including archiving, privacy and data protection, police powers and administration, freedom of information, criminal law, and the law of evidence. Search results that dealt with things other than law enforcement or administration, or with a very narrow topic, were discarded; for example, the *Gas Services Information Act 2012* (WA) which deals with 'access' by the relevant Minister to 'information' and 'documents' in 'possession' of the Independent Market Operator in that State.

Once relevant statutes were identified, the authorised version of each was trawled either by reading start to finish (where the document was not searchable) or by performing a search on each of the linking terms and on the information entities terms (data, information, record, document) (where the document was searchable). In doing these searches, we identified additional terms that were used to link entities and information. We performed the same 'trawling' process for each of these newly discovered linking terms in the statute in which they were found. If the newly discovered linking term was not a 'combination' term (in the last row of Table 1 below), we re-trawled all other statutes for instances of that term.

All of the linking terms – those of which we were aware at the outset and those we found in trawling the legislation – are set out in Table 1 below. The categories were

25 Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Australian Crime Commission Amendment (National Policing Information) Bill 2015 [Provisions]*; *Australian Crime Commission (National Policing information Charges) Bill 2015 [Provisions]* (Report, March 2016) 13–14 [2.15]. See also CrimTrac, Submission No 12 to Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into the Future Impact of Serious and Organised Crime on Australian Society* 9.

26 Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into the Gathering and Use of Criminal Intelligence* (Report, 15 May 2013) 75 [6.1], 79 [6.15]; Department of the Prime Minister and Cabinet, *Roadmap* (n 15) 2, 5–6.

selected in attempt to group similar terms, tying them to a common theme, each of which is explained below:

- Property, which covers terminology usually found in property law;
- Collection, which refers to the fact that an entity obtained or received information;
- Obligation, which denotes responsibility;
- Availability, which denotes accessibility to the entity;
- Physical, which involves an analogy with a hand's grasp or is associated with something the entity physically controls;
- Influence, covering the term control;
- Custody, which, through analogy with child custody, suggests influence and obligation. This term did not fit easily into other categories;
- Combinations that link together words in different categories through conjunction or layering of definitions. Layered definitions (indicated in the table as 'defined as' or 'includes' according to the manner of definition) are when one term is defined in terms of other terms within the Act. Where a term is defined exclusively (and not simply as including) terms that are otherwise all in the same category, the new term is included in that category. This is so even if the defined term might otherwise belong to another category, as where the term control is defined exclusively in terms of responsibility.

Table 1: Terminology Used in Legislation Linking Australian Law Enforcement Agencies to Information

Category Most Closely Associated with	Terms
Property	**possess/possession**; **property**; owned; of [entity]; its
Collection	**acquire**; **obtain**; gain; comes to knowledge; produce to; given to; disclosed to; made or received; recorded, collected or obtained; created by, obtained by or given to; obtained or created; creates or obtains possession; collects or handles; kept; originated from and is more closely related to; comes to knowledge or into the possession of (where possession includes control)
Obligation	**responsible for**; care; control meaning responsible for keeping
Availability	**access**; **has/had access to**; reasonably practical to obtain; available to; has or can reasonably obtain; possession defined as entitled to; held/hold, defined to include entitled to access or immediate right of access; has or can reasonably acquire; had reasonable access
Physical	**hold**; **held**; **holding**; **holder**; in a [name of entity] database; held or used
Influence	**control**
Custody	**custody**
Combinations	document of an agency defined in terms of possession, whether created or received; document of an agency defined using possession, control and access; control or entitled to control meaning possession or entitled to possess; control meaning possession or custody; held, holds or holding, defined to include possession or control and entitled to access (from private sector); held, holds or holding, defined as possession or control; collected or held; collected, held, managed, used, disclosed or transferred; obtained, received or held; holds information in computer storage; possession and power; possession or power; possession includes control; possession includes custody or control; possession or control; possession or control, with control defined in terms of possession or control; possession, custody or control; possession, custody or power; care, defined in terms of custody; custody or control; control of the custody; control, meaning possession, custody or power; made and kept; made and kept or received and kept; responsible for meaning entitled to control including made and kept or received and kept and possession or custody; held, defined as possession or control or responsible for; created or received or taken control of

Relevant provisions for *all* linking terms are set out in Table 2.[27] The provisions are colour coded – blue indicates an allocation of responsibility and red an allocation of power. Where neither is the case directly (as in the case of definitions that are used for both purposes) or a provision simultaneously allocates powers and responsibilities, purple is used. Linking terms are grouped by broad themes that are discussed in Part IV; where terms from more than one theme are combined, they are categorised as 'composite' in the table.

27 Available at <http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2020/04/who-owns-information-table.pdf>.

In some cases, 'information' is not the term used *in the actual provision*, but rather another term is used that includes at least some kinds of information. For example, many statutes use terms such as 'documents' or 'records' which are then defined in a way that includes either information generally[28] or specific[29] kinds of information (such as maps, plans, drawings and photographs).[30] Checking which terms include information (or electronic files, which are in a similar situation) involves reviewing interpretation legislation in addition to definition provisions in the substantive Acts being analysed.[31] In some Acts, the term 'record' or 'document' was defined in a way that excluded information from the definition; in such cases, associated provisions are not included in the table.[32]

The purpose of this task is not necessarily to be comprehensive. It is also beyond the scope of this article to explore the interpretation of each term in each statute in depth. Rather, the function of the table is to illustrate that the terminology used to link entities to information in the context of the case study is unnecessarily diverse. This provides a doctrinal base that explains some of the confusion that arises in practice in Part V. Even if some statutory linking terms can be interpreted by legal experts and given specific meanings in the contexts of cloud computing and data sharing platforms, the diversity of terminology makes it practically difficult to do this comprehensively. The table also forms a base from which to extract useful categories for building the taxonomy in Part VI.

---

28 *Federal Court Rules 2011* (Cth); *Public Governance, Performance and Accountability Act 2013* (Cth); *Police Act 1990* (NSW); *Privacy and Personal Information Protection Act 1998* (NSW); *State Records Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW); *Government Information (Public Access) Act 2009* (NSW); *Crimes Act 1958* (Vic); *Health Records Act 2001* (Vic); *Victoria Police Act 2013* (Vic); *Criminal Code Act 1899* (Qld); *Police Service Administration Act 1990* (Qld); *Rules of the Supreme Court 1971* (WA); *Police Act 1892* (WA); *Criminal Code Act Compilation Act 2013* (WA); *Information Privacy Principles (IPPS) Instruction* (SA); *Health Records (Privacy and Access) Act 1997* (ACT); *Territory Records Act 2002* (ACT); *Freedom of Information Act 2016* (ACT); *Information Act 2002* (NT).

29 *Australian Federal Police Act 1979* (Cth); *Freedom of Information Act 1982* (Cth); *Archives Act 1983* (Cth); *Privacy Act 1988* (Cth); *Evidence Act 1995* (Cth); *Evidence Act 1995* (NSW); *Uniform Civil Procedure Rules 2005* (NSW); *Public Records Act 1973* (Vic); *Freedom of Information Act 1982* (Vic); *Evidence Act 2008* (Vic); *County Court Civil Procedure Rules 2008* (Vic); *Magistrates' Court General Civil Procedure Rules 2009* (Vic); *Privacy and Data Protection Act 2014* (Vic); *Supreme Court (General Civil Procedure) Rules 2015* (Vic); *Evidence Act 1977* (Qld); *Public Records Act 2002* (Qld); *Information Privacy Act 2009* (Qld); *Right to Information Act 2009* (Qld); *Evidence Act 1906* (WA); *Freedom of Information Act 1992* (WA); *State Records Act 2000* (WA); *Evidence Act 1929* (SA); *State Records Act 1997* (SA); *Supreme Court Civil Rules 2006* (SA); *District Court Civil Rules 2006* (SA); *Magistrates Court (Civil Division) Rules 1998* (Tas); *Supreme Court Rules 2000* (Tas); *Evidence Act 2001* (Tas); *Right to Information Act 2009* (Tas); *Personal Information Protection Act 2004* (Tas); *Crimes Act 1900* (ACT); *Court Procedure Rules 2006* (ACT); *Evidence Act 2011* (ACT); *Information Privacy Act 2014* (ACT); *Evidence (National Uniform Legislation) Act 2011* (NT); *Police Administration Act 1978* (NT).

30 For example, the *Acts Interpretation Act 1901* (Cth) s 2B defines 'document' in a way that includes information. However, the *Public Records Act 1973* (Vic) only includes 'information' in the definition of a 'public record' where it is in the form of a map, plan, drawing or photograph. Because information *can* be included in the definition, terms linking 'public records' to entities in Victoria are included (and similarly for other examples).

31 *Acts Interpretation Act 1901* (Cth) s 2B; *Interpretation of Legislation Act 1984* (Vic) s 38; *Interpretation Act 1984* (WA) s 5; *Interpretation Act 1987* (NSW) s 21; *Legislation Act 2001* (ACT) Dictionary pt 1; *Interpretation Act 1978* (NT) s 17.

32 For example, relevant provisions in *Freedom of Information Act 1991* (SA) (with one exception where terminology is unclear, that is s 4(5), where information may be referred to in circumstances where a 'document' [physical medium] can be produced on the basis of stored information); *Rules of the Supreme Court 1971* (WA); *Police Service Administration Act 1990* (Qld); *Right to Information Act 2009* (Qld); *Information Privacy Act 2009* (Qld); *Archives Act 1983* (Cth) were excluded.

III IMAGINING OWNERSHIP OF INFORMATION

The law enforcement community includes individuals with two different understandings of what 'ownership' of information might mean. Each of these two conceptions of ownership comes with common means of identifying the entity that 'owns' information and articulating the consequences of that ownership. In particular, ownership as an allocation of power or control over information generally suggests a single owner, whereas ownership as the allocation of responsibilities for information may involve multiple owners. This suggests that, rather than searching for a coherent conception of information ownership, what matters is clarity around the rules for allocating the power to make decisions with respect to information and allocating responsibilities for information.

When asked about *which entity* owned information and about *what ownership entails*, research participants split into those who identified the owner as a single agency who had collected, created or bought the information (20) and those who identified as owners all agencies who had obtained the information (4). Some participants (7) used different words for each (with terms such as custodian, part owner, carer or borrower for those obtaining information from another entity). With the question of what ownership entails, participants associated the term 'ownership' of information with the exercise of control over that information (making decisions about who could use it and for what purposes) (7), the taking of responsibility with respect to that information (for example, ensuring it was stored securely, destroyed when required, etc) (10), or both (9). Both power and responsibility arise, for example, where there is a power that must be exercised subject to responsibilities. Interestingly, only one participant described all agencies who had obtained the information (whether named as owners or custodians) as having some power to make decisions with respect to it; such agencies were seen by most participants as having responsibilities as a result of having obtained information.

A Ownership as Control

Some participants associated ownership primarily with *the right to make decisions* respecting information. For all of these, the *owner* of information was exclusively or primarily the *creator* or *original collector* of that information. Ownership arose from 'authorship', having 'purchased it', or from the fact that the record was 'created or collated' or 'sourced or created' by a particular agency. There are echoes of property here, particularly of the everyday view of property,[33] as well as Katz's theory that focuses on owners as agenda-setters for a resource.[34] Examples of participants discussing a creator or originator's 'ownership' of information being the ability to make decisions respecting information include:

> [Name of organisation] owns it if it generated the data. It can decide who uses the information and in what context. OC05
>
> Some of it we will own because we have generated it – we have created it. Other information we would have purchased. … So if someone from [name of unit] gives me a piece of info[rmation] I can't give it to [name of organisation] without asking first. PC16

33 See Paul Babie, Peter D Burdon and Francesca Da Rimini, 'The Idea of Property: An Introductory Empirical Assessment' (2018) 40(3) *Houston Journal of International Law* 797 (empirical study based on semi-structured interviews with a range of people living in Adelaide, Australia).

34 Larissa Katz, 'Exclusion and Exclusivity in Property Law' (2008) 58(3) *University of Toronto Law Journal* 275, 278.

For participants who conceived of ownership primarily in terms of *control over information*, if the initial agency sent a copy of the information to another agency, the initial agency retained the power to determine how it was used. According to a number of participants (13), this had consequences for on-disclosure and the re-use of that information, sometimes due to provisions in memoranda of understanding. This was also important where the information was seized from an individual, in which case the data subject has residual rights (for example to have the data returned or destroyed), although vis-à-vis other agencies, the agency which collected it has ownership. For example:

> The owning agency has to have actually given permission for me to use it for the purposes I want to use it for. AC21
>
> Understanding that it is not ours to give and we should be contacting the owner of that agency and letting them know what is going on. I use it (the information) but understand it's not mine. PC11
>
> [T]here still does need to be an understanding that if you access information and you then wish to use it, that you need to seek approval from that agency. … [O]nce you've got that information and you then want to use it for a purpose, you need to talk to [name of originating agency] first. P03
>
> If someone shares [with] you data for a particular purpose, that you can't then go and use it for another purpose or without their permission … P13

Nevertheless, one participant opined that those who had received data from an originating agency did have some powers with respect to it:

> [I]t['s] probably better described as we've become custodians of information from time to time. … Ownership of data? No, I don't think it's the right term. Allowed to see it and allowed to manage it for purposes, yes. P10

Some participants also acknowledged that sharing data could result in a practical loss of control, even though they technically remained 'owners'. One participant suggested that ownership could be transferred from a legal perspective.

Where new intelligence products are created out of old ones, participants associating ownership with control generally believed that the derived product is 'owned' by the creating agency, although as some participants pointed out, the distinctions can be complex:

> I guess it's about when you share it and then they create new data or information or intelligence out of it then the agencies that did that work owns the new data or the new intelligence. … They don't own the source data but they've now created something else out of that. So then the people who have done that, or the agency that's done that work owns that new piece. P08
>
> We don't own our data. We own our information reports and other material gathered through examination. AC03
>
> There is a big difference between asking [name of organisation] 'Does this person have a criminal history?' and they say 'Yes' and I put it into my database and then I own it. But if I release an [name of organisation] intelligence report and it has an author then it is theirs – we never own it. OC13

Those who identify ownership with having control over information generally believe that information is 'owned' by the entity that created, collated or sourced it. This entity continues to 'own' it despite providing that information to a second entity, although this may diminish the extent to which the original agency can, in practice, control the information. However, a second agency may receive information from the first agency, incorporate it into a new product (such as an intelligence report), which may then be owned by the second agency.

B Ownership as Responsibility

While the picture of ownership described above suggests a consistent set of rules, it does not align with the views of those who view ownership of information primarily as aligned with responsibility for it. These participants generally saw the idea or an idea of information 'ownership' as closely related to the question of which agency had *responsibility* for that data. This included some who linked 'ownership' with creation and thus, like the group who associated ownership with control, treated the agency which created the information as also having the responsibilities associated with it:

> [Q: What do you think it means for an agency to own information?] Responsibilities are the first thing I thought of. Once you are imposed with ownership of information you are also imposed with the responsibility of the protection of that information – not only the protection of it but the appropriate use of it which must include pragmatic sharing of it. PC20

> I suppose there is a sense of ownership … in that you're forced to follow rules that dictate what you can do with it. … I would imagine it means having governance around that which is things around how long it's stored for, where it's sorted, protection to that data, making sure that there's appropriate controls around it not being lost or stolen or hacked in some way. O09

However, other participants allocated ownership of, or responsibility for, data to anyone who had a copy of that data:

> I think we own information where we generate it – where we are responsible for it. And where we received it in line with those particular caveats then use it accordingly. Once someone has given it to you then of course you own it. And if you give it to someone else it is a shared responsibility. OC13

> It becomes our information if we obtain it and retain it in my view. PC08

This has a different impact than limiting ownership to the generally singular entity that first created, captured or generated the information. Here, ownership is a many-to-one relationship, so that multiple entities will have responsibilities for the same information. This point was made explicitly by one participant in relation to freedom of information laws:

> If there's a person that lodges an FOI with [name of organisation] and a person that lodges an FOI with us regarding that same bit of information, both agencies need to make a determination about how they're going to respond to that. Generally, we consult on it but each agency's got to make their own assessment. P03

Thus, the lens of ownership as responsibility can suggest (although not necessarily) that there are multiple owners of information, each with independent responsibilities. The same point if one discards the term 'ownership, as suggested by PC17, and simply focuses on allocating responsibility.

IV THE COMPLEXITY AND INCONSISTENCY OF STATUTORY CONCEPTIONS OF INFORMATION AND ITS RELATIONS

As Tables 1 and 2 reveal, there is a plethora of words and expressions used to link entities and information. This diversity is itself problematic, as it complicates agencies' ability to know which decisions can or must be made with respect to which data. In addition, some of the terms used are themselves inappropriate or confusing. For example, the fact that information is not property makes it difficult to interpret legislation that refers to information that is an agency's property or in an agency's possession (section A). Physical terminology, such as 'hold' are inappropriate for that which cannot be grasped (section B). Finally, some terminology is used in ways that are circular (section C). Nevertheless, there are important distinctions made in existing

legislation that should be preserved in any new taxonomy (section D). Analysing these challenges provides a useful doctrinal context for the practical challenges in interpreting existing law in the context of new data practices, an issue that will be addressed in Part V.

A Property Terminology Should Be Limited to Media on which Information Is Stored

Property law is a standard mechanism for linking people and 'things' for the purpose of allocating rights, powers and responsibilities. It is the owner of a horse, for example, who can decide who rides the horse, has the power to sell the horse, and has the responsibility to take care of it.[35] While there are different interpretations of the meaning and purposes of the concept of property which are beyond the scope of this article, there are two important points to draw out. The first is that property involves some physical or conceptual thing.[36] The second is that the reluctance to treat information as property stems from its lack of exclusivity, commonly identified as a core attribute of property.[37] Exclusivity is considered important because it is the context in which interests come into conflict.[38] The exclusivity test maintains that a thing can only be the object of property if it cannot be simultaneously held and transferred or taken by another. Thus property generally[39] signifies a one-to-one relationship between entities and things.

While most resources fall under the doctrines of property law, information is not itself an object of property rights. In Australia, courts have stated this in a variety of contexts.[40] In *Federal Commissioner of Taxation v United Aircraft Corporation*, the High Court held that income derived under an agreement 'for the communication of information which would facilitate the manufacture of [aircraft] engines in Australia' was not derived from any 'property' in Australia.[41] Latham CJ's judgment was clear in its refusal to treat information as a form of property that could be the subject of a bailment or transfer,[42] stating explicitly that '[k]nowledge is valuable, but knowledge is neither real nor personal property'.[43] Other cases have echoed his view.[44] The issue of

35 For an example of responsibilities assigned to the owner of an animal, see *Prevention of Cruelty to Animals Act 1979* (NSW) ss 4 (definitions of 'person in charge', 'owner'), 8 (noting that this responsibility may also apply to others in addition to the owner).

36 See, eg, Henry E Smith, 'Property as the Law of Things' (2012) 125(7) *Harvard Law Review* 1691; JE Penner, 'The "Bundle of Rights" Picture of Property' (1996) 43(3) *UCLA Law Review* 711.

37 *Breen v Williams* (1996) 186 CLR 71, 90 (Dawson and Toohey JJ); MG Bridge, *Personal Property Law* (Oxford University Press, 4th ed, 2015) 3; William Cornish, David Llewelyn and Tanya Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (Sweet & Maxwell, 8th ed, 2013) 37–42 [1-41]–[1-46]; R Grant Hammond, 'Quantum Physics, Econometric Models and Property Rights to Information' (1981) 27(1) *McGill Law Journal* 47, 54. Cf Law Commission, *Misuse of Trade Secrets* (Consultation Paper No 19, 25 November 1997) 19 [3.19].

38 Christopher M Newman, 'Using Things, Defining Property' in James Penner and Michael Otsuka (eds), *Property Theory: Legal and Political Perspectives* (Cambridge University Press, 2018) 69, 90.

39 Exceptions are co-ownership and trusts, which have their own doctrines.

40 Incidentally, information is also not patentable subject matter: *D'Arcy v Myriad Genetics Inc* (2015) 258 CLR 334, 372–3 [93]–[94] (Gageler and Nettle JJ).

41 (1943) 68 CLR 525, 533–4 (Latham CJ).

42 Ibid.

43 Ibid.

44 See, eg, *Moorgate Tobacco Co Ltd v Philip Morris Ltd [No 2]* (1984) 156 CLR 414, 441 [34] (Deane J) ('it had long been the common law that, in the absence of rights of patent, trade mark or copyright, information and knowledge are not the property of an individual'); *Brent v Commissioner of Taxation (Cth)* (1971) 125 CLR 418, 425–7 [8]–[10] (Gibbs J) (in particular '[n]either knowledge nor information is property in a strictly legal

the classification of information arose in *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* ('*Farah Constructions*') where the High Court held that liability would only be imposed where the defendant could be shown to have received 'property',[45] and information that 'in the public domain' was not property.[46] Echoing Latham CJ in *Federal Commissioner of Taxation v United Aircraft Corporation*, the Court in *Farah Constructions* opined that even secret information would not generally be property, although it did suggest that 'trade secrets' share characteristics with property, given that they can be held in trust and charged.[47] In *Denlay v Federal Commissioner of Taxation*, data that may have been 'derived' from an offence was 'information' and hence not property for the purposes of proceeds of crime legislation.[48] The Court also noted that the physical discs on which the data was stored were 'property' and were, therefore, capable of being the proceeds of crime.[49]

The only category of information that has been described as a kind of property is trade secrets. In particular, rights to 'trade secrets' have sometimes been treated similarly to property, leading some to argue that property is the appropriate legal framework for understanding rights to information.[50] Equity provides that a person who learns of confidential information in circumstances where he or she has notice that, or has agreed that, the information is confidential is usually bound by an obligation of confidence.[51] The right can operate against third parties who receive the information indirectly[52] or who obtain the information surreptitiously.[53] The law of confidence has also borrowed heavily from property law in identifying the owner of trade secrets.[54] The relationship between the equitable obligation of confidence and the idea that confidential information is property was explored in the Federal Court case of *Smith Kline Laboratories*, where Gummow J stated:

> The degree of protection afforded by equitable doctrines and remedies to what equity considers confidential information makes it appropriate to describe it as having a

sense'); *Federal Commissioner of Taxation v Sherritt Gordon Mines Ltd* (1977) 137 CLR 612, 630 (Jacobs J) ('the possessor of the "know-how" has no right in it against the world'); *Pancontinental Mining Limited v Commissioner of Stamp Duties (Qld)* [1989] 1 Qd R 310, 311 (de Jersey J) ('the ordinary meaning of the word [property] does not encompass information').

45 (2007) 230 CLR 89, 145 [121] (Gleeson CJ, Gummow, Callinan, Heydon and Crennan JJ) ('*Farah Constructions*').

46 Ibid 143–4 [117]–[119].

47 Ibid 144 [118].

48 (2011) 193 FCR 412, 431–2 [68]–[74] (The Court).

49 Ibid 432 [72].

50 Sam Ricketson, 'Confidential Information – A New Proprietary Interest? Part II' (1978) 11(3) *Melbourne University Law Review* 289.

51 *A-G (UK) v Guardian Newspapers [No 2]* [1990] 1 AC 109, 281–2 (Lord Goff).

52 *Prince Albert v Strange* (1849) 1 H & TW 1; 41 ER 1171; *Federal Commissioner of Taxation v United Aircraft Corporation* (1943) 68 CLR 525, 535–6 (Latham CJ); *Fraser v Evans* [1969] 1 QB 349, 361 (Lord Denning MR).

53 *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 224 [34] (Gleeson CJ), 289 [223] (Callinan J); *Franklin v Giddins* [1978] Qd R 72, 80 (Dunn J); *Shelley Films Ltd v Rex Features Ltd* [1994] EMLR 134, 147–8 (Martin Mann QC); *Creation Records Ltd v News Group Newspapers Ltd* (1997) 39 IPR 1, 7–8 (Lloyd J); *Ashcoast Pty Ltd v Whillans* [2000] 2 Qd R 1, 6 (McPherson JA).

54 The same result will not hold for other types of confidential information: JD Heydon, MJ Leeming and PG Turner, *Meagher, Gummow & Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 5th ed, 2015) 1172–3 [42-120].

> proprietary character. This is not because property is the basis upon which that protection is given, but because of the effect of that protection.[55]

Trade secrets are thus not things in which the plaintiff has a proprietary interest, but they are protected in a similar way to such things because of requirements of conscionable dealing.[56] Thus trade secrets, like the broader category of confidential information, are not objects of property rights, although there will be remedies available to plaintiffs who claim a breach of the equitable obligation of confidence.

While information is *not* property, Table 1 illustrates that a number of statutes use property language to link entities and information, including the word 'possess'.[57] These laws do not *create* property rights in information,[58] but rather *assume* them in allocating powers and responsibilities.

The problem here is not the inconsistency between general law (the fact that information cannot be property) and statutory terminology (suggesting information is property or can be possessed) per se. After all, there is no difficulty in the idea that statutes use particular terms in ways that are inconsistent with the meanings of those terms under the general law.[59] Further, these statutes are not the only context in which the concept of 'possession' is applied to information – criminal law does this in the context of specific offences,[60] including identity theft laws,[61] insider trading laws,[62] and possession of child abuse material.[63] In all of those situations, courts interpret the relevant provisions when called to do so in light of principles of statutory interpretation, including by reference to legislative purpose. Interestingly, many common law courts' interpretations to date have been context-specific, so that one might be in 'possession' of insider trading information if one is aware of it,[64] but not in 'possession' of child abuse material unless it is consciously downloaded or saved with a degree of permanence beyond transient display on a screen.[65]

---

55 *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services & Health* (1990) 22 FCR 73, 121 (Gummow J) ('*Smith Kline Laboratories*'). See also *Moorgate Tobacco Co v Philip Morris Ltd* (1984) 156 CLR 414, 438 (Deane J) ('[l]ike most heads of exclusive equitable jurisdiction, its rational basis does not lie in proprietary right. It lies in the notion of an obligation of conscience arising from the circumstances in or through which the information was communicated or obtained'); *Breen v Williams* (1996) 186 CLR 71, 129 (Gummow J) ('[n]or is it acceptable to argue that … the plaintiff who asserts an obligation of confidence therefore has proprietary rights in the information in question which in turn found a new species of legal right').

56 See also *Mid-City Skin Cancer & Laser Centre Pty Ltd v Zahedi-Anarak* (2006) 67 NSWLR 569, 620–1 [235] (Campbell J); *TS & B Retail Systems Pty Ltd v 3fold Resources Pty Ltd* (2007) 158 FCR 444, 464 [75] (Finkelstein J); *Elecon Australia Pty Ltd v Brevini Australia Pty Ltd* (2009) 263 ALR 1, 58 [262] (Buchanan J) (upheld in *Elecon Australia Pty Ltd v PIV Drives GmbH* (2010) 93 IPR 174).

57 'Property' and 'possession' are closely aligned concepts: see generally *Jeffries v The Great Western Railway Company* (1856) 119 ER 680.

58 Lothar Determann, 'No One Owns Data' (2018) 70(1) *Hastings Law Journal* 1.

59 *Wik Peoples v Queensland* (1996) 187 CLR 1.

60 *Warner v Metropolitan Police Commissioner* [1969] 2 AC 256, 304 (Lord Pearce); *Towers & Co Ltd v Gray* [1961] 2 QB 351, 361 (Lord Parker CJ); Alex Steel, 'The True Identity of Australian Identity Theft Offences: A Measured Response or an Unjustified Status Offence?' (2010) 33(2) *University of New South Wales Law Journal* 503; Alex Steel, 'Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property' (2008) 30(4) *Sydney Law Review* 575.

61 See, eg, *Criminal Code Act 1995* (Cth) s 372.2; *Crimes Act 1900* (NSW) s 192K.

62 *Corporations Act 2001* (Cth) s 1043A.

63 See, eg, *Crimes Act 1900* (ACT) s 65.

64 *R v Hannes* (2000) 158 FLR 359, 397–8 [227]–[230] (Spigelman CJ). See also *R v Farris* (2015) 301 FLR 230, 272 [169] (Hall J).

65 *R v Morelli* [2010] 1 SCR 253, 266 [18], 270 [30] (Fish J), 303 [137] (Deschamps J); *Atkins v DPP (UK)* [2000] 2 All ER 425; *R v Porter* [2007] 2 All ER 625; *Clarke v The Queen* (2008) 185 A Crim R 1, 55 [246] (Barr J); *R*

There is also no difficulty in the idea that information may be property for the purposes of a specific statute or treaty, but not for the purposes of the general law. In *Dixon v The Queen*, the Supreme Court of New Zealand found that there was no need to reconsider the 'orthodox view' that 'pure information is not property' in deciding that 'digital files' held on a USB were – for the purpose of the statutory offence of 'dishonest acquisition of property from a computer system' under *Crimes Act 2003* (NZ) section 249(1)(a) – 'property'.[66] While the Court of Appeal had treated digital files as 'pure information',[67] and thus not property, the Supreme Court interpreted the term 'property' in its legislative context as including digital files because they 'are "things" in which a person has an "interest"', 'have a physical presence' and 'can be identified, have a value and are capable of being transferred to others'.[68] This interpretation relied on legislative history and purpose,[69] and the Court also observed that it was consistent with the common conception of property.[70] There are other circumstances in which confidential information has been treated as being property, for example in the interpretation of 'possessions' in Article 1 of the First Protocol of the European Convention on Human Rights.[71] This reflects the fact that terms in statutes may be interpreted, in context, in ways that are inconsistent with general law meanings.

However, given the lack of a concept of possession of, or property in, information at common law, any interpretation of statutes employing this concept will need to draw on the statute's own purpose and context in explaining that interpretation. That interpretation may well be different to an agency's assumptions, articulated in contracts or memoranda of understanding with other agencies. As in the case of criminal law, this may mean that an entity will have 'possession' of information for some statutes but not for others. Such complexity has the potential to sow confusion among agencies grappling with application of the government's data governance and public transparency framework in an evolving information technology environment.

An additional problem with using property language is that, traditionally, it suggests a one-to-one relationship between entities and things. Outside the concept of co-ownership (which has its own rules), only one entity can have 'possession' of a 'thing'. As pointed out in Part II, the lack of exclusivity is one reason why courts have refused to recognise property in information for the purposes of the general law. At the same time, many-to-one relationships with information are becoming increasingly common, for example in the context of cloud computing and the NCIS. Using language that suggests a search for a single 'owner' is inappropriate here. However, property is the correct concept to describe relationships between entities and physical media on which information is stored (for example, computer servers). Those physical media may be the property of a law enforcement agency or may be the property of a third-party provider (as with cloud computing).

---

v Daniels (2005) 191 CCC (3d) 393, 397 (Welsh JA). See also *Littlejohn v Hamilton* (2010) 199 A Crim R 63, 71 [17] (Porter J).

66 [2016] 1 NZLR 678, 690–1 [23]–[25] (Arnold J for the Court).

67 Ibid 689 [18]–[19].

68 Ibid 690–1 [25], 691 [29].

69 Ibid 691 [27]–[29], 693 [33].

70 Ibid 698 [51].

71 *R (Veolia ES Nottinghamshire Ltd) v Nottinghamshire County Council* [2010] EWCA Civ 1214; [2011] LGR 95, 135 [121] (Rix LJ). See also discussion in Tanya Aplin, 'Confidential Information as Property?' (2013) 24(2) *Kings Law Journal* 172, 176, noting that interests that are not classified as private property may nevertheless be characterised as 'possessions'.

While property language is not useful in linking entities to *information*, it can be used to link entities to physical media on which information is stored, such as the physical discs in *Denlay v Federal Commissioner of Taxation*.[72]

B Terms That Assume Physicality Are Unhelpful

The verb 'to hold' and its derivatives suggest a physical grasp of an object, so are potentially confusing when used in relation to information. A file in a filing cabinet can be physically grasped or physically controlled (through access to the filing cabinet). But determining which entity 'holds' information stored on a server in the cloud pursuant to a contract granting control and/or access to different entities requires an assessment beyond physicality. Many of the statutes using these terms define them in terms of other terms (such as possession and control). The term 'possession' is not useful for the reasons explained above, although the term 'control', if well defined, may be (discussed in Part IV(D)). Nevertheless, the physicality of the verb 'to hold' means that it does not add anything useful in this context.

C Circularity of Terminology

Obligation-related terms such as 'care for' or 'responsible for' are used less frequently in legislation relevant to the case study, although they are sometimes used to describe the relationship between archiving agencies and archival records. For example, 'responsibility' is the term that links a person to a document or thing with respect to which they are entitled to give evidence,[73] which is interesting because it creates a link between the allocation of responsibility (presumably external to evidence law) and the allocation of a specific power (to give evidence). It can also be the case that a power hinges on care lying with a third-party entity.[74] However, obligation-related terms will generally be circular when used to describe responsibilities for information,[75] as it effectively defines responsibility in terms of responsibility. Further, it will be rare that powers will be dependent on pre-existing obligations.

Circularity is also a potential problem when influence-related terms are used to identify an agency with powers over information. However, when the term 'control' is used in some archiving and privacy legislation, it is to allocate specific responsibilities, such as amending information, protecting records, granting access to records, and transferring records. The concept of 'control' is thus used in an attempt to find the *one* entity which will ensure that certain things happen. The term 'control' is a useful influence-related term that can link responsibilities to entities with practical control over information. However, it is circular to allocate rights of control to entities with existing control.

The term 'custody' is used more broadly[76] and, while it also suggests a measure of influence, it could, by analogy with child custody, include elements of responsibility. It is sometimes used for allocating powers[77] and sometimes for allocating

72 (2011) 193 FCR 412, 431–2 [68]–[74].

73 See, eg, *Evidence Act 1995* (NSW) s 171.

74 See, eg, *Archives Act 1983* (Cth) s 69.

75 This seems to be the case in respect of the examples from *State Records Act 2000* (WA).

76 The breadth is demonstrated in the colour coding used in the Appendix (see, in particular, the provisions shown in red, which indicate a provision allocating power to control).

77 See, eg, *Archives Act 1983* (Cth) s 28 (the entitlement of the Archives to access depends on the 'custody' of the records, defined in a way that includes information).

responsibilities,[78] and even in rare cases to outline the responsibilities of third parties.[79] Indeed, four research participants used the term 'custody' to describe entities with responsibilities for data. Thus, 'custody' is potentially a more ambiguous term than 'control', as it could be applied to the entity with physical possession of the medium on which information is stored, the entity with day-to-day control of it, or any entity that has responsibilities with respect to it. Depending on its interpretation in the context of specific legislation and whether powers or responsibilities are allocated on the premise of custody, the term may be circular. However, its multiple potential meanings make it less useful as a basis for linking entities and data on a one-to-one basis.

D Useful Distinctions in Existing Terminology

Collection-related terms, such as acquire and obtain, can be many-to-one and are thus potentially useful for imposing certain kinds of responsibilities on entities. For example, secrecy and confidentiality provisions such as in the *Territory Records Act 2002* (ACT) and *State Records Act 1998* (NSW) should apply to anyone who has obtained (or acquired) certain kinds of information. Collection-related terms are also useful in prescribing what can be done with information, as in the case of *Criminal Code* (WA) section 83, which deals with corruption.[80] However, while there is a wide variety of terms that fall into the collection category, it is not clear that they draw meaningful distinctions in substance. Simplicity would suggest a single term. One possibility would be the term 'to obtain' (currently the most popular), while another would be to embrace a broader term such as 'to process' (a term used in the European Union's General Data Protection Regulation and defined in article 4(2) as meaning any operation performed on information).[81]

Availability-related terminology is used in situations where responsibilities are assigned to entities which *could* access information, even if specific information has not been accessed. For example, the concept of 'entitled to access' is used in defining when information is 'held' in *Freedom of Information Act 2016* (ACT) section 14. This ultimately creates an obligation to grant access to information that *could* be accessed by certain ACT agencies. In the context of the increasing use of data-sharing platforms, it is likely unhelpful, and promoting of entity-shopping, to allocate responsibilities that need only lie with *one* entity to every entity that *could* obtain access. In practice, it may also reduce the willingness of other jurisdictions to grant such agencies access to their information. However, there are some circumstances in which there should be obligations to produce information that an agency can access, as in the context of particular investigations. Availability-related terminology is also appropriate in formulating rules as to when specific access can be obtained (for example, when an authorisation is required).

Perhaps most problematic are some of the ways in which terms are combined. For example, where control is defined in terms of possession or control and then linked again with the term possession in any event, creating a tripled layering of definitions.[82] The sheer range of combinations, within and across jurisdictions, adds to the difficulty

78 See, eg, ibid s 31 (requiring co-operation with Archives to make certain records publicly available).

79 See, eg, ibid s 36 (obligation to provide access in a particular form affected by impact on entity with custody).

80 *Criminal Code Act Compilation Act 1913* (WA) sch 1 s 83 ('*Criminal Code*').

81 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016* [2016] OJ L 119/1, art 4(2).

82 See, eg, *Information Privacy Act 2009* (Qld) s 24. See also other provisions in Table 2 at n 27.

for an entity seeking to develop clear policies and practices for managing obligations or appropriately exercising powers relating to information. At most, there may be a need for a provision to apply on the basis of a term in one category and a term in another (for example, a responsibility to put security protocols in place may apply to an entity that has possession of the physical media on which information is stored and to an entity that has the ability to access the information).

Based on the legislation reviewed in Table 2,[83] it appears that distinctions need to be drawn between powers and responsibilities allocated on the basis of which entity has the ability to access information, which entity has accessed or processed information, which entity has control over information, and which entity has possession of the physical media on which information is stored. In the case of personal information, there is also the entity to whom the information pertains. While current laws include terms that make these distinctions, the terminology is excessively diverse, rendering the network of laws concerning ownership of information unnecessarily complex.

V PRACTICAL CHALLENGES OF CONFUSED OWNERSHIP: INFORMATION SHARING IN LAW ENFORCEMENT

While the previous Part described a technical legal problem, this Part will return to the interview data to explore the practical impact of unclear laws in the context of the case study, namely the law enforcement community and the challenge of information sharing. Laws that link information with entities through property language need to be applied on a daily basis by a variety of entities, especially those responsible for distributing and accessing information across the law enforcement community. There are particular challenges as agencies seek to modernise and automate information storage and information sharing practices. This Part focuses on responses in interviews to questions concerning the extent to which confusion about 'ownership' created practical problems for cloud computing and the NCIS pilot. This confusion is evident in the diversity of interpretations among research participants, as well as the uncertainty they express as to the control retained over data.

A Cloud Computing

Participants were asked specifically about how they conceived of ownership where information was stored in the cloud. Some participants (8) responded by saying that the service provider owns information uploaded to the cloud:

> Whoever owns the server. All the cloud is a server. Whichever agency holds that information owns that. PC14
>
> The person who owns it is actually the cloud host because that is who I will speak to to get the cloud data if it is possible. PC16
>
> I don't want to be cynical – the IT companies that created the cloud ultimately own it only because nine-tenths of the law is possession. I think they own it: we just place it there. PC20

Others (11) saw it as simply a storage facility, with ownership resting with the originating agency who contracts with a cloud service provider:

83 See above n 27.

> It is no different – the ownership arrangements don't change whether the server is at the end of the room or on the other side of the world as far as I am concerned. The agency that generated the information owns it. PC19
>
> The cloud is a storage device. If you use a storage facility to take all your stuff from your back room and put it in a storage facility – Wilson's Storage. They own the storage facility: you own what's in it. If you put stuff in the cloud you are leasing that space. They don't have a right to that data, they have the right to the lease and the rent. OC06

Several noted that the concept of cloud ownership was generally unclear:

> I would still say that we would own it but a lawyer would disagree with me and the people who own the cloud might disagree with me. OC07
>
> I honestly couldn't speak to what sort of data we have that's in that sort of environment. I'd like to say that there's very little, I know I'd be lying. P12
>
> Cloud storage is an area of law that I've particularly avoided because it's just too abstract for my way of thinking. P14

The inconsistency of views and lack of clarity around control over, and responsibility for, information stored in the cloud presents risks, as some participants observed:

> There is a big risk of reputational damage to the agency ... And identity theft and data breaches are also reputational issues for us … OC04
>
> I think the government has a responsibility for the information – they own it, they are choosing to store it in the cloud. But also you would want to hope that there is some knowledge of which server that is being stored on and which protections are around that space to make sure its security and integrity and accessibility is maintained. AC10
>
> I am not opposed to cloud storage but I do worry when there is a third party I guess involved. PC11

Although these observations were not based on interpretation of specific statutory or contractual provisions, they indicate confusion 'on the ground' about the link between entities and information stored in the cloud. As participants pointed out, lack of clarity here can result in risk, particularly where responsibility for data governance is unclear.

B Shared Data Platform (NCIS)

Participants were asked directly about who owns the information accessed through a shared data platform to which different law enforcement agencies would have access (such as in the context of the NCIS trial). Some suggested the information is owned by the platform itself. One participant (P01) believed that the *Australian Constitution* implied that all information passing over a Commonwealth system was owned by the Commonwealth. However, many participants stated confidently that it was the agency providing or uploading information which owned it (which is not necessarily the originating agency). A consequence of this, noted by one participant, is that 'you might have several owners of the data that is returned to you'. One participant proposed a quite different set of relationships, placing control and responsibilities such as archiving with the 'originating agency' and other responsibilities with everyone who 'utilises' the information:

> [Data on the platform is owned by] [t]he originator of the data who's putting it onto the … platform and the person who accesses that information – so the end user, end holder and then the user. … [I]t should be a process where there is an archiving by the owner because they are the original owners. If the end users are going to utilise that information then they accept the responsibility of being the end users as well. PC08

Consistently with the view set out above, PC14 felt that ownership was with the entity that has 'got control of that cloud or server', being ACIC. One participant

expressed the view that 'once it is in [the data platform], it's everybody's data' but qualified this by noting that protections needed to be in place, for example in relation to ongoing investigations (P04). Another participant expressed a similar view, stating 'If an agency has placed their data in the NCIS, it will be assumed they want to share' (AC21).

The concept of ownership, in terms of either control over information or obligations with respect to it, is difficult to apply to cloud storage and shared data platforms. There appear to be inconsistent views among research participants, suggesting that there is still legal uncertainty among relevant agency personnel. Given the importance of ensuring clarity around who is responsible for storing, securing, archiving, updating, protecting and disclosing information stored in the cloud or on shared data platforms such as NCIS, greater precision of language is required.

C Implications for Data as a National Asset

In both conceptions of ownership, ownership as *control over information* and *responsibilities with respect to information*, most (30) participants viewed information as 'owned' by an agency or by a small group of agencies. A few dealt specifically with the idea that information should be a 'national asset', a common mantra in policy recommendations in Australia and elsewhere,[84] for example noting that 'at the macro level it belongs to all of us' (AC02). There was little opposition to the philosophy of greater information sharing across the law enforcement community, although participants often referred to legislative requirements as a barrier:

> At the moment, we're promoting interoperability and asset management, digital processes and whole of government use of government information. … [B]ut our legislation at the moment and other government policies present obstacles to information sharing. O07

> We will be happy to share and can see the advantages of sharing if government said you're allowed to share. So, there's no ownership there, it's around people just trying to follow the rules that are there. O09

Both of these research participants present legislation or 'the rules that are there' as barriers to information sharing. This does not mean that the legislation is in fact a barrier, but that it is perceived as such. Complexity can contribute to this; simple and clear rules that facilitate appropriate sharing are more likely to be used than complex exceptions to secrecy requirements, particularly by those who *want* to increase information sharing. Where there is a significant volume of relevant legislation governing control over and responsibility for information (as per the previous Part), that may also reduce willingness to risk acting contrary to a legislative requirement.

In addition to real or perceived legislative constraints, participants pointed to obligations to international partners, 'need to know' particularly in the context of current investigations, and the need for responsibility over data to be located somewhere as barriers to removing concepts of agency 'ownership'. Thus, even if 'ownership' was collective, 'management' (including making decisions about information and taking on associated responsibilities) needed to lie somewhere more concrete. For example:

---

84 See 'Australian Government Public Data Policy Statement' (n 2) 4. In the United States, see Markle Foundation, *Mobilising Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment* (Third Report, July 2006) 45 ('there should ... be an explicit statement of policy that originators or producers [of information] do not own or control the information they produce'); Transcript of Hearing, *Federal Support for Homeland Security Information Sharing: Role of the Information Sharing Program Manager (*House of Representatives, 109th Congress, Lee H Hamilton, 8 November 2005) 24.

> I don't know that there needs to be an originating owner. I think information ought to be more of a collective notion. Information … for want of a better term … ought to be owned by all appropriate law enforcement bodies. It is really how it is managed that is the issue. P20

This kind of specific allocation of information to entities need not be inconsistent with the idea of information as a 'national asset', at least in the sense that it is shared whenever appropriate. Ownership was sometimes described as a connection between an agency and particular data or information that was necessary *so that appropriate information sharing could occur*. For example:

> The obligations of owning data are to make sure that it is stored appropriately. *And that if someone needs it you share it with them* and conversely that you restrict it appropriately. (emphasis added) AC03

> [Ownership] [d]oesn't mean we shouldn't share or have data as a national asset. P08

> Shared resources still must have a single point of authority. O07

In addition, as OC06 pointed out, data integrity requires ownership for verification. Further, as P01 noted, it is difficult to determine which agency needs to field freedom of information requests.

In fact, most participants believed that allocation of ownership to particular agencies (or individuals within those agencies) was a *facilitator* rather than an *obstacle* to greater information sharing. Thus, despite visions of treating information as a 'national asset', there remains a need for allocation of control over information and allocations of responsibility for information to specific agencies (or officers within those agencies). Generally speaking, it may make sense for the former to be a one-to-one relationship while the latter needs to operate as a many-to-one relationship. Clarifying these roles and reducing complexity can, in the view of at least some research participants, enhance appropriate information sharing. For example:

> I mean you would simplify the legislation and not have nine or seven different evidence Acts across the country and things like that. [Interviewer: Are there ways around that problem?] I mean if the Commonwealth introduced overarching legislation. As long as there was some strict criteria. P15

> I think a unified system would be ideal. I think that we would be far more able to, I guess, comply with our legislative obligations if (1) we knew everything that we held – which I don't believe we currently do – and understood where everything was at any given time, then that would allow us to actually effectively manage our information, which I don't know that we currently do. P18

It is worth noting here that legislation that promotes information sharing does not necessarily address the gap created by lack of clarity about 'ownership'. For example, the *Data Sharing (Government Sector) Act 2015* (NSW) still requires consideration of which entity 'controls' data, as defined in that Act.[85] It assumes that the identification of that entity occurs based on external facts; it does not say who the controller is, only what the controller must do. Similar issues are likely to arise with Commonwealth data sharing and release reforms, as discussed in the following Part.

85 *Data Sharing (Government Sector) Act* (NSW) ss 4(1) (definition of 'government sector data'), 4(2). The definition there implies that an entity will have 'control' if it has possession or custody of the data or if it 'has' the data in the possession or control of another entity.

VI PROPOSED REFORMS

This Part outlines two modes of law reform that may help solve current information sharing challenges. These are specific new legislation to authorise and encourage information sharing (section A) and greater clarity about links between information and entities (section B). It concludes that the former, where most current government efforts are concentrated, is less likely to be successful in the absence of the latter.

A Government Reform Proposals

Since the Productivity Commission published its report on *Data Availability and Use*,[86] the federal government has been investigating ways in which information sharing can be enhanced. In March 2019, the Minister for Human Services and Digital Transformation released a report entitled *Sharing Data Safely*.[87] This repeats the view that 'data is a significant national asset' and outlines existing practices, data sharing principles and public sector data reforms.[88] The report includes a description of five data sharing principles, equivalent to the 'Five Safes' framework used by the UK Data Service,[89] which sets out the questions that should be asked about various matters including the nature of the data sharing project, the identity and trustworthiness of people involved, the environment in which data is accessed, the protections in place and level of detail for data, and the identifiability of outputs. These are a prelude to the development of new data sharing legislation aimed at 'improving governance and transparency of Commonwealth data sharing' which will incorporate the Data Sharing Principles as a 'key component'.[90] This new legislation is now the subject of a Discussion Paper, released in September 2019.[91]

None of these principles, even if formalised in legal instruments, assists with the challenges identified in this article. First, the Discussion Paper confirms that data sharing for law enforcement and national security purposes will not be permitted under the new legislation.[92] The complex legislation that underlies these protections is thus preserved in the proposed data sharing framework.

Even aside from specific exclusions, there remains the crucial question of clarifying *which entity* has control over the information in order to make decisions under data sharing legislative frameworks. In a *Best Practice Guide to Applying Data Sharing Principles*, the Department of Prime Minister and Cabinet has set out some new definitions.[93] The relevant one, '[d]ata [c]ustodian', is defined as '[t]he agency that collects or generates data for any purpose, and is accountable and responsible for the governance of that data'.[94] This is similar to the definition in the Discussion Paper, which is relevantly:

---

86 Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 8 May 2017).
87 Office of the National Data Commissioner, *Sharing Data Safely* (Report, March 2019).
88 Ibid.
89 Information on this framework is available at 'Regulating Access to Data', *UK Data Service* (Web Page) <https://www.ukdataservice.ac.uk/manage-data/legal-ethical/access-control/five-safes>.
90 Office of the National Data Commissioner (n 87).
91 Australian Government, Prime Minister and Cabinet, 'Data Sharing and Release: Legislative Reforms Discussion Paper' (September 2019).
92 Ibid 14, 21, 23, 25.
93 Department of the Prime Minister and Cabinet, *Best Practice Guide to Applying Data Sharing Principles* (Guide, 15 March 2019).
94 Ibid 4.

> Data Custodians are Commonwealth entities and companies as defined under the *Public Governance, Performance and Accountability Act 2013*, such as agencies and departments, including Commonwealth companies such as Australia Post and NBN. Data Custodians collect or generate public sector data for the purpose of carrying out their functions and have legal responsibility to manage this data.[95]

There are several problems with such definitions. First, the term 'custodian' is not ideal for the reasons set out in Part IV(C) above. Second, the conjunction 'and' in both versions of the definition is ambiguous, for example in situations where an agency collects data but enters into a memorandum of understanding with a second agency to store it and fulfil governance responsibilities with respect to it. Third, what is important here is knowing which agency to approach in relation to data access, that is a one-to-one relationship, whereas the definition could reveal multiple agencies that are simultaneously 'custodians', creating a risk of forum shopping. Finally, the proposal adds a new concept and definition into a morass of terminology, so that the entity connected to information for the new legislation may be different to the entity otherwise exercising powers over and taking responsibility for information in other contexts.

The reforms may well assist agencies to make better decisions about the circumstances in which data is shared, but without clearer terminology will not assist to identify the data over which they have authority to make such decisions. Data sharing legislation would thus be enhanced if it incorporates clearer terminology for describing entity-information relationships in the context of allocating powers to make decisions with respect to data.

B A Taxonomy to Capture Relationships with Information

The challenges faced in the context of law enforcement in assigning information to entities for the purposes of allocating control and responsibilities no doubt apply elsewhere. Much of the legislation considered in Part IV applies to government more broadly and some also applies to elements of the private sector. If this is a problem worth solving, it is worth solving across the board.

This section proposes a new taxonomy to capture relevant relationships with information. Because it draws on a specific case study, it may need to be supplemented by other terms that are important in other contexts. In this sense, it is offered as the beginning of a clarification process.

There are more fine-grained distinctions that can be drawn among different relationships entities might have with information. Perhaps the most comprehensive is the Data Management Body of Knowledge framework.[96] The technical distinctions drawn in that document go beyond what appears necessary for the case study considered here, particularly given the way that roles are often aggregated within particular entities. Certainly, the morass of words currently used in legislation do not correspond to any fine distinctions that might be drawn but reflect a more haphazard approach.

The first kind of relationship that an entity may have with information is if it is entitled to access that information. An entity may be able to access particular information (either generally or conditionally), but not necessarily have the ability to add to, change or destroy the underlying information.[97] An entity may never in fact access particular information, despite its ability to do so. The information that it can

95 Australian Government (n 91) 55.

96 The Data Management Association, *DAMA-DMBOK2 Framework* (Framework, 6 March 2014).

97 An example of this is in *Archives Act 1983* (Cth) s 28.

access may also be different from the information that exists – for example an entity may only be able to access metadata (such as the fact that another entity has information in relation to a particular person) or part of an information file. Entities with a mere right to access rarely have control over the relevant information. The responsibilities of such entities are likely to be limited to those framed in terms of the circumstances in which access (which may itself be limited) is permitted. There may, in addition, be circumstances when an entity is under an obligation to obtain access to documents, as is the case for some freedom of information requests in the ACT and may also be the case for discovery in litigation.[98] However, creating such responsibilities (in statute or otherwise) may have negative implications on the willingness of third-party organisations to provide such access. In particular, an agency may decline to make information accessible to another agency where the second agency thereby comes under an obligation to share the information publicly, at least where the first agency was under no such obligation in their own jurisdiction.

The second kind of relationship that an entity may have with information is that they have processed the information in some way. This includes having acquired it, created it, or otherwise obtained it, but also incorporates other uses of information such as using it, consulting it or deriving new or altered information from it.[99] It goes beyond having an ability to access information to having accessed it. When entities which can access information do so, additional responsibilities may come into play. For example, there may be a requirement to keep it secret or comply with limitations as to how it can be used, whether set by the entity from which the information was obtained or by statute. In the existing statutory taxonomy described in Part IV above, the main terms used are 'acquire' and 'obtain', although there are many others. Typically, entities obtaining information do so in order to 'use' it in some way. There is thus a need for a term such as 'process' to capture situations where information is created, viewed or used by an entity. This term can then be linked to responsibilities (including restrictions on use and requirements in secrecy and privacy laws). In processing information, an entity may also create new information (for example, extracting individual suspects or threats from a larger data set) or make a copy thereof. The entity may take on different roles in relation to this derived or copied data as suggested in Part III(A) (for example, it may exercise control over it). Generally speaking, any relevant powers (beyond powers of use, copying and derivation) would attach to the copied or derived information in the entity's role as controller.

That brings us to the third kind of relationship, where an entity has control over information, in the sense that it can add to, change, copy or destroy data within a particular category within legal limits, whether or not it has possession of the physical medium on which the data is stored. There is some Australian precedent for defining

98 On the former, see *Freedom of Information Act 2016* (ACT) s 14 (discussed in Part IV above); on the latter, see *Susquehanna International Group Limited v Needham* [2017] IEHC 706, [51] (Baker J) (although, in that case, the defendant had a statutory right to the information). In Australia, a party may be required to discover documents in its 'power': see, eg, *Federal Court Rules 2011* (Cth) r 20.1, Dictionary (definition of 'control').

99 A useful definition, from art 4(2) of the European Union's *General Data Protection Regulation* defines processing as

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

control in terms of power.[100] In the context of information, control will often be limited by statutory obligations (such as those in privacy and data protection laws and archiving laws). Any definition of control or controller would thus need to be stated in terms of powers that apply subject to other laws. By default, this could be specified as the entity initially creating or obtaining information. The distinction between the second and third categories is subtle but important in that a controller can change the original data, whereas a processor does not have this power. Where a processor alters the data, this creates 'new' data over which the processor will generally have control. Allocating responsibilities to those with control over information is appropriate where there is a need for a one-to-one relationship between entities and information, as is the case with archiving legislation.

As explained in Part II, information is not property that can be 'possessed'. However, an entity may have possession of the physical medium on which information is stored ('possess' in relation to the *physical* medium). While only one entity would have possession of one physical medium, multiple entities could have possession of physical media storing the same data. Possession of chattels is a well-established common law concept[101] and thus would not need to be defined, provided that it is only used in relation to tangible things such as hard drives, servers and paper files. Possession of physical media may be important in the allocation of some responsibilities (for example, to ensure data integrity and security).

There are other roles that could be relevant in particular contexts. For example, a platform provider may, but need not, have the ability to access the data available on its platform (for example, where encryption is used or internal access is otherwise restricted) and it may, but need not necessarily, have possession of the servers on which data are stored. Unless an entity providing a platform, software or service has the ability to access unencrypted information, control over information or possession of physical servers, responsibilities for information per se will be few. Of course, there may be general obligations to comply with discrimination law and government accountability and transparency rules, and contracts may require particular security measures. There would unlikely be any need, however, for powers or responsibilities of the kind set out in Table 2 to be allocated to such entities unless they fulfilled one of the roles already discussed.[102]

The main terms that are needed for most legislation linking entities and information for the purposes of allocating rights, powers and responsibilities are thus 'has access to', 'process', 'control' and 'possession' (in relation to the physical medium) or synonyms of these terms. Using these more specific and appropriate terms, legislation would be able to articulate and distinguish rights, powers and duties that entities have in relation to information. For example, data controllers could be allocated responsibility for archiving and freedom of information requests and primary responsibility for data protection, possessors could be allocated primary responsibility for physical security of servers, while secrecy and confidentiality obligations could be linked specifically to processing information.

100 *Federal Court Rules 2011* (Cth) Dictionary (definition of 'control').

101 To have possession of a tangible thing, a person must control that thing and intend to possess it. For a summary of the meaning of possession, see generally Robert Chambers, *An Introduction to Property Law in Australia* (Lawbook Co, 4th ed, 2019) ch 5.

102 See above n 27.

There are, of course, intersections among many of these roles. A data aggregator can be thought of as combining the above depending on the context (perhaps entitlement to access and possession but not control). Entities may take on different roles for different data – an entity may have mere access to data A but use it to derive data B which they store locally (thus taking on control of the new derived data and possession of the medium on which that new data is stored). Derived data may thus have different entities associated with them than the original data.

There are choices in which kind of relationship is the appropriate one for the allocation of a specific power or responsibility. While the ACT links freedom of information explicitly to the ability to access information, this may be a disadvantage in circumstances where it reduces the willingness of other jurisdictions to share their information. An alternative is for freedom of information requests to be directed at the most relevant agency (likely the data controller). Similar questions arise for discovery. But these decisions are matters of policy; the goal here is focused on development of a taxonomy through which such debates can take place.

VII CONCLUSION

Although there is no property in information, there is a need for clarity around which entities can make decisions about the use of information (subject to law) and which entities have particular responsibilities (often specified by statute) for information. This is particularly evident in law enforcement, where a complex legislative regime based on inconsistent and sometimes confusing terminology is one of the barriers to information sharing. This article has begun the task of developing a clear taxonomy to replace the miscellany of terms appearing in legislation that allocates specific powers or responsibilities to specific entities. The taxonomy may be incomplete because it was constructed in the context of a case study; other relationships to information may be important in other contexts. More work may be required to test and apply the taxonomy in particular statutes. However, it is hoped that this exercise is a useful way to begin considering important policy questions, including a clear allocation of responsibility for data governance, archiving obligations and transparency requirements. Such clarity in the 'ownership' of information will enhance rather than undermine the goal of ensuring that government information can be appropriately deployed for national benefit in areas such as law enforcement.