DATA SHARING AGREEMENTS: CONTRACTING PERSONAL INFORMATION IN THE DIGITAL AGE

SHIRI KREBS* AND LYRIA BENNETT MOSES†

Voluminous information about individuals is being shared every day and everywhere. Streamlining data sharing activities effectively allows public and private entities to use information for policy advancement, knowledge creation and business growth. At the same time, such sharing of personal information also risks harming individuals' privacy and autonomy. How are data sharing activities governed in Australia? What are the main problems with the existing legal framework? This article explores three ways in which the interests of individuals whose data is being shared may be better protected. These are (a) improvements in data privacy and data sharing legislation, (b) adapting private law frameworks to create more protective structures (as in the notion of 'data trusts' and 'information fiduciaries') and (c) enhancing data governance through better contracts, including model data sharing agreement templates. We conclude that while law reform may be desirable, particularly along the lines of the first possibility, organisations that truly 'care about privacy' can act now to improve their data sharing practices through better data sharing agreements and the data culture that they cultivate. The Australian Office of the National Data Commissioner can lead the way with a restructured and reimagined data sharing model agreement.

CONTENTS

* Professor of Law and Director of the Centre for Law as Protection, Faculty of Business and Law, Deakin University.

† Professor and Head of the School of Law, Society and Criminology, Faculty of Law and Justice, University of New South Wales. The work has been supported by the Cyber Security Cooperative Research Centre whose activities are partially funded by the Australian Government's Cooperative Research Centres Program. We would like to thank the *Melbourne University Law Review*'s Editorial Board for their thorough and diligent editing suggestions and Sanjay Alapakkam for his research assistance.

I Introduction

Data 'sharing' between organisations is an increasingly common practice that takes place in a variety of contexts. Data is shared in the contexts of the sale of business, the sale of data to raise funds, data broking and subscription services, policy development, pandemic response, the development of artificial intelligence systems, building smart cities and law enforcement.[1] Increasingly,

[1] Shiri Krebs and Lyria Bennett Moses, 'Data Sharing Agreements: Contracts for Access to Personal Information in the Digital Age' (SAO Seminar, Data61 and Cyber Security Cooperative Research Centre, 9 December 2021) 0:01:41–0:02:00 <https://webcast.csiro.au/#/videos/e31d9ae6-4db9-4008-a49f-a6e722f23ce1>. See also 'Selling

data sharing activities by both public and private entities involve the transfer of, or access to, personal information.[2] As larger volumes of personal information are shared more widely and frequently, risks to data privacy, integrity and security, as well as to human rights, also increase.[3] However, despite the

a Business', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/selling-a-business>, archived at <https://perma.cc/57Y2-P7ZK>; 'Trading in Personal Information', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/trading-in-personal-information>, archived at <https://perma.cc/QF5H-J3FN>; Information Commissioner's Office (UK), *Data Sharing Code of Practice* (Code, 17 October 2022) 61 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice-1-0.pdf>, archived at <https://perma.cc/VTH4-ZQWU> ('*UK Agreement*'); *Data Availability and Transparency Act 2022* (Cth) s 15(1)(b) ('*Cth DAT Act*'); *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments* (Agreement, 9 July 2021) <https://federation.gov.au/sites/default/files/about/agreements/iga-data-sharing-signed.pdf>, archived at <https://perma.cc/WN8K-PNUR> ('*Intergovernmental Agreement*'), discussed in Senate Select Committee on COVID-19 (Cth), *Final Report* (Report, April 2022) 66 [4.53] <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024920/toc_pdf/Finalreport.pdf;fileType=application%2Fpdf>, archived at <https://perma.cc/T2SS-5RFF>; Productivity Commission, 'Making the Most of the AI Opportunity: AI Raises the Stakes for Data Policy' (Research Paper No 3, January 2024) 4–5 <https://www.pc.gov.au/research/completed/making-the-most-of-the-ai-opportunity/ai-paper3-data.pdf>, archived at <https://perma.cc/LA54-RVXN> ('AI Opportunity'); Sidewalk Labs, *Digital Governance Proposals for DSAP Consultation* (Draft Proposal, October 2018) 10, 12–13 <https://www.waterfrontoronto.ca/sites/default/files/documents/18-10-16-swt-draft-proposals-regarding-data-use-and-governance-tuesday-730pm.pdf>, archived at <https://perma.cc/9J4Z-8JXK>; *Privacy and Data Protection Act 2014* (Vic) sch 1 cls 2.1(e), (g) ('*Vic Privacy Act*').

[2] The meaning of 'personal information' is defined in the federal and equivalent state and territory privacy legislation: *Privacy Act 1988* (Cth) s 6(1) (definition of 'personal information') ('*Cth Privacy Act*'); *Information Privacy Act 2014* (ACT) s 8(1) ('*ACT Privacy Act*'); *Privacy and Personal Information Protection Act 1998* (NSW) s 4 ('*NSW Privacy Act*'); *Information Act 2002* (NT) s 4A ('*NT Information Act*'); *Information Privacy Act 2009* (Qld) s 12 ('*Qld Privacy Act*'); *Personal Information Protection Act 2004* (Tas) s 3 (definition of 'personal information') ('*Tas Information Protection Act*'); *Vic Privacy Act* (n 1) s 3 (definition of 'personal information'); *Freedom of Information Act 1992* (WA) Glossary cl 1 (definition of 'personal information') ('*WA Freedom of Information Act*'). The link between the concepts of 'data' and 'information' (including personal information) is rarely made clear in legal discussions, although the link is sometimes made clear in information science: see, eg, Michael K Buckland, 'Information as Thing' (1991) 42(5) *Journal of the American Society for Information Science* 351, 351–4; Lothar Determann, 'No One Owns Data' (2018) 70(1) *Hastings Law Journal* 1, 6.

[3] See, eg, Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017) 8–11, 57–60 <https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf>, archived at <https://perma.cc/V9K9-BQ2Y> ('*Data Availability*'); Moira Paterson

substantial growth in the sharing of personal information in Australia and globally, Australian regulation of data sharing activities provides only partial protection against the harms linked with data sharing activities.[4]

Following significant regulatory developments in recent years (especially in Europe),[5] emerging literature on data sharing, both domestic and comparative, tends to focus on the regulatory mechanisms governing data sharing activities.[6] But government regulation is not the only mechanism through which data sharing activities are governed. In this article, we develop a contract-based data governance approach to data sharing and holistically explore the regulatory and contractual mechanisms that regulate data sharing activities. Our 'data governance approach' includes not only the laws that dictate how data is collected, processed, used and shared but also the organisational system of decision-making roles, duties and accountabilities for data sharing processes.[7] While these decisions are not typically governed or mandated by law, they still hold immense significance for how data is shared and the effects of sharing activities on the people whose data is shared.[8] A 'data governance approach',

and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1, 6–9.

[4] Kate Galloway, 'Big Data, Government, Privacy and Human Rights' in Paula Gerber and Melissa Castan (eds), *Critical Perspectives on Human Rights Law in Australia* (Lawbook, 2021) vol 2, 357, 357–9.

[5] See *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*'); *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724* (*Data Governance Act*) [2022] OJ L 152/1 ('*DGA*'); *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)* [2023] OJ L (22 December 2023) ('*Data Act*').

[6] See, eg, Paterson and McDonagh (n 3) 2; Inge Graef and Bart van der Sloot, 'Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving beyond Individual Empowerment' (2022) 33(4) *European Business Law Review* 513, 514–17; Oscar Borgogno and Giuseppe Colangelo, 'Data Sharing and Interoperability: Fostering Innovation and Competition through APIs' (2019) 35(5) *Computer Law and Security Review* 105314:1–17, 2–4.

[7] See also Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) 131(2) *Yale Law Journal* 573, 579, 634–53.

[8] Our approach is consistent with critical data studies literature, which supports the idea that data governance structures should go beyond formal legal standards and include informal and soft law instruments: see, eg, Rachelle Bosua et al, 'Using Public Data to Measure Diversity in Computer Science Research Communities: A Critical Data Governance Perspective' (2022) 44 (April) *Computer Law and Security Review* 105655:1–10, 7–10.

therefore, concerns both the overarching data sharing principles and the concrete decisions that should be made to ensure effective management and use of data (including determining who is qualified and responsible to make such decisions).[9] It prescribes the source of authority for making decisions about data processing, the roles, structures and processes adopted to make such decisions, and the basis upon which such decisions should be made.[10] Importantly, a 'data governance approach' to data sharing guides the operationalisation of the legal rules in everyday decision-making practices and it mitigates any gaps between legal obligations and data sharing practices, generating an organisational culture that is sensitive to the interests of — and potential harms to — individuals and groups whose data is being collected and shared.[11] Data governance is also an important 'bedrock' for artificial intelligence governance.[12]

Our analysis of the legal mechanisms that do or could govern domestic data sharing activities in Australia identifies three types of mechanisms. First, we engage with the emerging literature in this field by noting recent developments in this ever-changing regulatory regime, including data privacy and data sharing legislation. In Australia, two core examples of such regulation are the *Privacy Act 1988* (Cth) ('*Privacy Act*') and the *Data Availability and Transparency Act 2022* (Cth) ('*DAT Act*'). Secondly, we note that in some jurisdictions and sharing contexts, data sharing may also be governed through property law mechanisms and structures such as trusts (noting, however, that it is unlikely that such mechanisms will be used in Australia).[13] Thirdly, we focus our attention on a core mechanism that governs most data sharing

[9] In this sense, our use of the phrase 'data governance' captures 'management' of data sharing arrangements. For an example of an approach incorporating both data governance and data management, see P Alison Paprica et al, 'Essential Requirements for the Governance and Management of Data Trusts, Data Repositories, and Other Data Collaborations' (2023) 8(4) *International Journal of Population Data Science* 01:1–23, 5–6.

[10] See, eg, Australian Institute of Health and Welfare, *Data Governance Framework 2021* (Report, 6 April 2021) 6–8 <https://www.aihw.gov.au/getmedia/a10b8148-ef65-4c37-945a-bb3effaa96e3/AIHW-Data-Governance-Framework.pdf.aspx>, archived at <https://perma.cc/4EHA-7FQX>.

[11] Viljoen (n 7) 578–9.

[12] Stefaan G Verhulst and Friederike Schüür, 'Interwoven Realms: Data Governance as the Bedrock for AI Governance', *Data & Policy Blog* (Blog Post, 20 November 2023) <https://medium.com/data-policy/interwoven-realms-data-governance-as-the-bedrock-for-ai-governance-ffd56a6a4543>, archived at <https://perma.cc/BX7X-4B34>.

[13] See below Part III.

activities yet has currently received little scholarly attention — contracts.[14] Data sharing activities are typically governed through bilateral or multilateral agreements between entities that share (or disclose) data and entities that gain access to data or receive copies of data.[15] While these agreements must operate within legal constraints, they offer an avenue to enhance protections beyond those already required by law — whether through replacing abstract principles with clear and concrete obligations or by adding additional requirements that are currently missing in the existing regulation.[16] To gain more insight into this diverse data sharing governance tool, we reviewed and analysed 23 publicly available data sharing agreements.

We find that, for data sharing within Australia, each of these three data governance mechanisms raises significant challenges. As we detail in Part II below, the relevant privacy legislation, which is currently under review federally, is limited in both scope and jurisdiction.[17] In particular, federal privacy law only covers the federal public sector and part of the private sector with respect to some of that sector's activities: for example, the federal law excludes employee records in some contexts while some states have very limited privacy regulation.[18] Given that data sharing can cut across federal and state public sectors and different parts of the private sector, federal privacy law does not apply to all data sharing activities within Australia. Inconsistency in language and terminology between state and federal law adds complexity, particularly given the ambiguity in the application of some terminology to new data practices.[19] The specific data sharing legislation (the *DAT Act*) is similarly insufficient to meet current challenges, as it contains general principles that fail to provide concrete and complete solutions to data sharing challenges.[20] Additionally, this legislation is context and entity-specific and is not capable of

[14] See below Part IV.

[15] Claudio Caimi et al, 'Legal and Technical Perspectives in Data Sharing Agreements Definition' in Bettina Berendt et al (eds), *Privacy Technologies and Policy* (Springer, 2016) 178, 182.

[16] These legal constraints are mainly imposed by data privacy and data sharing legislation: see below Part II(A).

[17] See Attorney-General's Department (Cth), *Privacy Act Review* (Report, 2022) 1 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>, archived at <https://perma.cc/S622-5KUG>.

[18] *Cth Privacy Act* (n 2) ss 6(1) (definitions of 'agency', 'APP entity' and 'employee record'), 6C(1), 7B(3). South Australia and Western Australia ('WA') do not have dedicated privacy legislation: see below nn 75–6 and accompanying text.

[19] See below n 64 and accompanying text. See also *Privacy Act Review* (n 17) 4, 302–3.

[20] See below Part II(A)(1).

harmonising data sharing responsibilities across different organisations, activities and jurisdictions within Australia.[21] This means that where data flows across sectors (between federal and state governments, between public and private sectors and to agencies subject to different rules such as national security and law enforcement agencies), the rules protecting data privacy and integrity change, complicating organisations' data sharing practices and curtailing the emergence of a rigorous data governance culture within data sharing entities.[22]

As for the property law route, the main challenge there is adapting frameworks that require identifiable property. As we detail in Part III(A) below, data is not subject to property rights in Australia thus limiting the possibility of further protections through property law mechanisms. There have been proposed workarounds, particularly in the context of data 'trusts', but these proposals are unlikely to achieve data governance objectives in Australia (including the simplification of data transfers and the protection of data privacy and integrity).[23]

Finally, while data sharing agreements can potentially fill some of the existing gaps in the existing regulation and provide tailored and concrete solutions to data sharing challenges, we find, as we elaborate in Part IV below, that they tend to include inaccurate and confusing terminology as well as incomplete provisions around data governance depending on the identity of the contracting entities and their interests. Greater standardisation, at least as an available option (like in real estate transactions), might thus enhance efficiency and improve data governance in practice.[24] Moreover, while serving as the main tool governing data sharing activities, data sharing agreements meaningfully affect third parties — mainly the individuals whose personal information is being shared ('data subjects') — without offering meaningful

[21] See below nn 60–4 and accompanying text. See also Productivity Commission, 'AI Opportunity' (n 1) 15–18.

[22] See Productivity Commission, 'AI Opportunity' (n 1) 15–18.

[23] See below Part III(B). See also BPE Solicitors, Pinsent Masons and Chris Reed, Queen Mary University of London, *Data Trusts: Legal and Governance Considerations* (Report, April 2019) 8 <https://www.bpe.co.uk/media/177005/24779-general-legal-report-on-data-trusts-digital v5-lr-final.pdf>, archived at <https://perma.cc/5CAV-RWKN> ('*Data Trusts*').

[24] See, eg, Law Society of New South Wales and Real Estate Institute of New South Wales, *Contract for the Sale and Purchase of Land 2022 Edition* (Contract, 2022) <https://www.lawsociety.com.au/sites/default/files/2022-09/Sample%20with%20 watermark_2022%20Land%20Contract_0.pdf>, archived at <https://perma.cc/8732-TMY5>. See below nn 213–17, 279 and accompanying text.

transparency to data subjects or formally including their interests in the contract negotiation process.[25]

Ultimately, the problems with all three mechanisms governing data sharing activities within Australia are that they generate suboptimal guidance for data sharing entities. Some of these deficiencies are legal or doctrinal in nature, while others are inherently governance problems.[26] Another type of deficiency relates to the gap between existing data sharing activities and individuals' expectations concerning their ability to control data flows and to protect their privacy.[27]

In this article, we explore whether and how the three data governance mechanisms described above — privacy and data sharing legislation, property law and contracts — might be adapted to better align with data governance objectives and data subjects' expectations of data sharing within Australia.[28] Part II explores the regulatory route to data governance; it briefly touches on recent developments in data privacy and data sharing legislation in Australia and considers law reform possibilities, including those inspired by legislative developments in the European Union ('EU'). Part III then analyses the existing — and potential — private law frameworks other than contract that may be utilised to improve data governance. In particular, these frameworks could include treating data as a kind of property, creating data 'trusts' or recognising information 'fiduciaries'. Part IV provides insight into the use of contracts as data governance mechanisms; this use adds another layer of concrete obligations that are consistent with and complement the regulatory guidance. Part V proposes methods to improve data governance through data sharing agreements. Finally, Part VI concludes by recommending potential avenues for law reform, but it focuses primarily on leveraging data sharing agreements *in the absence of such reform* to contract for better data governance. Even where this is not legally required, the proposed framework has benefits for managing risk, particularly around public confidence, reputation and

[25] See below Part IV.

[26] See below Parts II–IV.

[27] For example, 84% of Australians want more control and choice over the collection and use of their personal information, while 87% of Australians believe that selling or trading in personal information is not fair and reasonable: Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (Report, August 2023) 18, 52 <https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf>, archived at <https://perma.cc/K55B-4MXZ> ('*Community Attitudes*').

[28] Additional issues for cross-border data sharing are beyond the scope of this article.

goodwill. The federal government can, through its data sharing template agreement under the *DAT Act* scheme, lead the way.[29] We explain what such an approach will mean in practice and what data sharing agreements need to include for organisations committed to good data governance.

II Governing Data Sharing through Regulation

Australia's public sector entities engage in many data sharing activities.[30] These activities are governed by two kinds of legal framework: on the one hand, legislation focusing on privacy and data protection[31] and, on the other hand, data sharing or data availability legislation focusing on streamlining data flows.[32] This Part briefly considers the role played by Australian data privacy and data sharing legislation and how this legislation may be reformed for improved data governance.

A *The Australian Legal Approach to Regulating Data Sharing Activities: Streamlining Data Flows*

There are different possible approaches to government regulation of data sharing agreements: from a dignity-based approach focusing on protecting individuals whose data is being shared[33] to an approach that focuses on

[29] See below n 279 and accompanying text.

[30] See, eg, 'National Health Data Hub', *Australian Institute of Health and Welfare* (Web Page, 23 May 2024) <https://www.aihw.gov.au/reports-data/nhdh>, archived at <https://perma.cc/T7SD-S4LB>; 'How We Use Data Matching', *Australian Taxation Office* (Web Page, 15 May 2023) <https://www.ato.gov.au/about-ato/commitments-and-reporting/in-detail/privacy-and-information-gathering/how-we-use-data-matching>, archived at <https://perma.cc/8UFQ-AF6X>. See also Lisa Eckstein et al, 'Australia: Regulating Genomic Data Sharing to Promote Public Trust' (2018) 137(8) *Human Genetics* 583, 583–6. For data sharing in the private sector, see, eg, Natalia Jevglevskaja and Ross P Buckley, 'The Consumer Data Right: How to Realise This World-Leading Reform' (2022) 45(4) *University of New South Wales Law Journal* 1589, 1591–5, 1618.

[31] See, eg, *Cth Privacy Act* (n 2); *ACT Privacy Act* (n 2); *NSW Privacy Act* (n 2); *NT Information Act* (n 2); *Qld Privacy Act* (n 2); *Tas Information Protection Act* (n 2); *Vic Privacy Act* (n 1).

[32] See, eg, *Cth DAT Act* (n 1); *Data Sharing (Government Sector) Act 2015* (NSW) ('*NSW Data Sharing Act*'); *Public Sector (Data Sharing) Act 2016* (SA) ('*SA Data Sharing Act*'); *Victorian Data Sharing Act 2017* (Vic) ('*Vic Data Sharing Act*').

[33] In Germany, for example, data privacy rights are constitutionally protected as part of an understood basic right of 'informational self-determination': Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to

streamlining data between agencies to promote data as a public resource — this latter approach is becoming increasingly prevalent in Australia.[34] Data sharing legislation (such as the *DAT Act*) is designed to regulate data sharing activities that fall within the scope of the legislation,[35] while data privacy legislation is designed to protect personal information about individuals as well as data integrity and security.[36] Both kinds of frameworks vary significantly within Australia depending on the jurisdiction (whether federal, state or territory), the identity of the data sharing entity (eg whether public or private)[37] and the type of shared data (eg whether it involves personal or sensitive information).[38] As

Informational Self-Determination' (2009) 25(1) *Computer Law and Security Review* 84, 84–5. This right is a special part of Germany's general constitutional right of personality and can protect individuals against technological threats: at 86. While the right of informational self-determination does not create a right of absolute control over personal data, the Federal Constitutional Court of Germany extended meaningful constitutional protections over individuals' data privacy: at 84, 87. For additional details about the German approach to data privacy, see Paul M Schwartz, 'Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and New Technology' (2011) 53(2) *William and Mary Law Review* 351, 364–76. See also *Grundgesetz für die Bundesrepublik Deutschland* [Basic Law for the Federal Republic of Germany] arts 1(1), 2(1) ('*German Constitution*') [tr Christian Tomuschat et al, 'Basic Law for the Federal Republic of Germany', *Federal Ministry of Justice* (Web Document) arts 1(1), 2(1) <https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.pdf>, archived at <https://perma.cc/CJ3A-CW4X>]; Bundesverfassungsgericht [German Constitutional Court], 1 BvR 209/83, 15 December 1983 reported in (1983) 65 BVerfGE 1, 42–4 [tr 'Order of 15 December 1983: 1 BvR 209/83', *Bundesverfassungsgericht* (Web Page, 2023) [146]–[148] <https://www.bverfg.de/e/rs19831215_1bvr020983en.html>, archived at <https://perma.cc/Z4H5-J5DM> ('Order of 15 December 1983')].

[34] *Cth DAT Act* (n 1) ss 3(a), (e); *NSW Data Sharing Act* (n 32) ss 3(a)–(c); *SA Data Sharing Act* (n 32) ss 4(a)–(c); *Vic Data Sharing Act* (n 32) ss 1(b)–(c).

[35] That scope covers public sector data sharing: *Cth DAT Act* (n 1) s 3; *NSW Data Sharing Act* (n 32) s 3; *SA Data Sharing Act* (n 32) s 4; *Vic Data Sharing Act* (n 32) s 1.

[36] See, eg, *Cth Privacy Act* (n 2) s 2A; *ACT Privacy Act* (n 2) s 7; *NSW Privacy Act* (n 2); *NT Information Act* (n 2) s 3; *Qld Privacy Act* (n 2) s 3; *Tas Information Protection Act* (n 2); *Vic Privacy Act* (n 1) s 1.

[37] See, eg, *Cth DAT Act* (n 1) s 11; *NSW Data Sharing Act* (n 32) s 4(1) (definitions of 'data provider' and 'data recipient'); *SA Data Sharing Act* (n 32) s 3(1) (definitions of 'data provider' and 'data recipient'); *Vic Data Sharing Act* (n 32) s 3(1) (definition of 'data sharing body'). See also *ACT Privacy Act* (n 2) ss 9–11; *NSW Privacy Act* (n 2) ss 3(1) (definition of 'public sector agency'), 4(4); *NT Information Act* (n 2) ss 5–6; *Qld Privacy Act* (n 2) ss 17–18; *Tas Information Protection Act* (n 2) s 3 (definition of 'personal information custodian'); *Vic Privacy Act* (n 1) ss 13(1)–(2). Cf *Cth Privacy Act* (n 2) s 6C.

[38] See, eg, *Cth DAT Act* (n 1) ss 9 (definition of 'personal information'), 16A–16B; *NSW Data Sharing Act* (n 32) ss 4(1) (definition of 'personal information'), 11–15; *SA Data Sharing Act* (n 32) ss 3(1) (definition of 'personal information'), 7; *Vic Data Sharing Act* (n 32) s 3

we shall demonstrate below, both data sharing and data privacy legislation in Australia provide insufficient constraints on data sharing activities. Rather, most practical data governance lies in the promises that organisations extract from each other when negotiating data sharing agreements.[39]

We will first review the developing data sharing framework applicable to (some) data sharing agreements in Australia and then provide a brief overview of the current data privacy framework affecting (some) data sharing agreements.

1 *Data Sharing Framework*

At the federal level, data sharing legislation is evolving: the recent *DAT Act* is specifically designed to govern data sharing activities, particularly where personal information is involved.[40] The *DAT Act* aims to enhance and simplify the sharing of public sector data by Commonwealth entities by guiding the structure, content and availability of data sharing agreements.[41] To achieve this goal, the *DAT Act* specifies five broadly defined data sharing principles that provide general guidance for data sharing entities and activities.[42] The 'project principle' stipulates that a data sharing activity should consider the appropriateness of the program or project for which the data is shared, making sure that the program or project is expected to serve the public interest and to follow ethical processes.[43] The 'people principle' requires that shared data is made available only to appropriate persons and entities.[44] The 'setting principle' instructs that the environment in which the data is shared should be appropriately controlled and secured.[45] The 'data principle' requires that

(definition of 'personal information'). See also *Cth Privacy Act* (n 2) s 6(1) (definitions of 'personal information' and 'sensitive information'), sch 1; *ACT Privacy Act* (n 2) ss 8, 14 (definition of 'sensitive information'), sch 1; *NSW Privacy Act* (n 2) ss 4, 4A, 8–19; *NT Information Act* (n 2) ss 4 (definition of 'sensitive information'), 4A, 14, sch 2; *Qld Privacy Act* (n 2) s 12, schs 3–5; *Tas Information Protection Act* (n 2) s 3 (definitions of 'personal information' and 'sensitive information'), sch 1; *Vic Privacy Act* (n 1) s 3 (definition of 'personal information'), sch 1.

[39] See below Part IV(A).

[40] *Cth DAT Act* (n 1) pts 2.1–2.5.

[41] Ibid s 3. See also at pt 2.6.

[42] Ibid s 16.

[43] Ibid ss 16(1)–(2).

[44] Ibid ss 16(3)–(4).

[45] Ibid ss 16(5)–(6).

appropriate protections are applied to shared data.[46] The 'output principle' limits the outputs that result from data sharing and are based on shared data; additionally, this principle requires data sharing entities to consider the nature and intended use of planned outputs and to make sure that the final output contains only the data reasonably necessary.[47] These general principles are further explained and interpreted in the *Data Availability and Transparency Code 2022* (Cth), which provides guidance on these data sharing principles as well as privacy protections and best practices for data sharing.[48]

While these data sharing principles provide a general framework to guide data sharing entities in conducting their data sharing activities, the *DAT Act* perpetuates the main limitations of its predecessor (the *Best Practice Guide to Applying Data Sharing Principles*) by providing guidelines that only marginally instruct data sharing entities and agents.[49]

Beyond its generality, the *DAT Act* has some concrete limitations. First, the Act only recognises two types of entities within the data sharing ecosystem: 'data custodians' and 'accredited entities'.[50] Data custodians are defined as entities who control and 'hav[e] the right to deal with' public sector data; accredited entities are defined as those receiving access to public sector data and these entities can vary from users to data service providers from different sectors, including public sector, industry and research entities.[51] This focus on entities that control, access and share data omits data subjects and generates a data sharing environment or culture that focuses on the perspectives (and concerns) of the data sharing entities at the expense of the concerns and interests of the individuals whose personal information is being shared.

Secondly, the *DAT Act* places most of the responsibilities for data protection on the entity that 'holds' the data (defined, as in the *Privacy Act*, as an entity

[46] Ibid ss 16(7)–(8).

[47] Ibid ss 16(9)–(10).

[48] *Data Availability and Transparency Code 2022* (Cth) pts 2–3.

[49] See Department of the Prime Minister and Cabinet, *Best Practice Guide to Applying Data Sharing Principles* (Guide, 15 March 2019) 6, 13–28 <https://apo.org.au/sites/default/files/resource-files/2019-03/apo-nid225841.pdf>, archived at <https://perma.cc/8LDD-AXAF>; *Cth DAT Act* (n 1) s 16.

[50] *Cth DAT Act* (n 1) s 11. Some entities — mainly intelligence entities — are excluded from the scope of the *Cth DAT Act*: at s 11(3).

[51] Ibid ss 11(2), (4). See also Office of the National Data Commissioner, *Introducing the DATA Scheme* (Report, April 2023) 1–2 <https://www.datacommissioner.gov.au/sites/default/files/2023-04/Introducing%20the%20DATA%20Scheme%20-%20April%202023.pdf>, archived at <https://perma.cc/8TVM-B4M7>.

that 'has possession or control of a record that contains the personal information').[52] While this terminology follows the *Privacy Act*, it has been argued that this terminology is confusing and unhelpful in the context of digital data.[53] The term 'holds' often leads to confusion among individuals tasked with data sharing responsibilities as it connotes restrictive or physical control of data (notwithstanding formal legal interpretations of this term).[54] Instead, Australia should move towards a more modern terminology that distinguishes between entities that control data,[55] entities that process data, entities that have access to data and entities that possess the physical media on which data is stored.[56]

Thirdly, while this detailed data sharing framework successfully governs some aspects of data sharing agreements (such as the purpose and terms of the sharing activity or the security of shared data), it leaves other elements to be bilaterally (or multilaterally) negotiated and agreed upon.[57] For example, the *DAT Act* allows parties to authorise additional data sharing and to release data without placing clear legal constraints to effectively protect data privacy.[58] This is a direct result of adopting a 'data sharing principles approach' that does not mandate preferred data governance actions and instead includes a broad range of accepted activities and risk-mitigation practices.[59]

[52] *Cth DAT Act* (n 1) s 37(6); *Cth Privacy Act* (n 2) s 6(1) (definition of 'holds'). See also *Cth DAT Act* (n 1) ch 3. Although in cases of data breaches by accredited entities, if the public sector entity that shared this data with the accredited entity is aware of (or reasonably suspects) the breach, it is required to 'take reasonable steps' to prevent or reduce the harm and to undertake additional notification responsibilities: at ss 35–8.

[53] *Cth DAT Act* (n 1) s 37(6); *Cth Privacy Act* (n 2) s 6(1) (definition of 'holds'); Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion' (2020) 43(2) *University of New South Wales Law Journal* 615, 631.

[54] *Cth Privacy Act* (n 2) s 6(1) (definition of 'holds'); Bennett Moses (n 53) 631.

[55] Here, we refer to controlling data in the sense of decision-making power over the data, such as the power to modify it, and not necessarily in the European sense, which has been criticised: see, eg, Law Council of Australia, Submission No 594606615 to Attorney-General's Department (Cth), (27 January 2022) 22 [99] <https://lawcouncil.au/publicassets/ab940abf-57da-ed11-947f-005056be13b5/2023%2004%2013%20-%20S%20-%20Government%20Response%20to%20the%20Privacy%20Act%20Review%20Report.pdf>, archived at <https://perma.cc/D3UA-3YAP>. See also Bennett Moses (n 53) 639–40.

[56] Bennett Moses (n 53) 638–41.

[57] See *Cth DAT Act* (n 1) ss 18–19.

[58] Ibid ss 20A–20D.

[59] The 'data sharing principles approach' is based on the 'Five Safes' framework, which has been described as a 'structure and an ethos, helping to frame discussion': Tanvi Desai, Felix Ritchie and Richard Welpton, 'Five Safes: Designing Data Access for Research' (Working Paper

These problems within the existing (and evolving) data sharing regime limit its effectiveness in streamlining data sharing in the public interest while ensuring meaningful privacy protection.

In addition to the federal legislation, data sharing agreements between public entities in Australia are further regulated by state and territory legislation governing the sharing of data held by state and territory governments and agencies. For example, the *Data Sharing (Government Sector) Act 2015* (NSW), the *Public Sector (Data Sharing) Act 2016* (SA) and the *Victorian Data Sharing Act 2017* (Vic) ('*Victorian Data Sharing Act*') govern data sharing agreements between public entities within their jurisdictions and aim to remove impediments to the sharing of public sector data while maintaining concrete safeguards.[60] Each legislation has its own scope. For example, the *Victorian Data Sharing Act* applies specifically to data sharing 'for the purpose of informing government policy making, service planning and design' as well as for analytics purposes.[61] Some — but not all — state laws require the consideration of privacy legislation and of other legal obligations.[62] Further, only South Australia ('SA') explicitly requires the consideration of policies related to data governance (the 'trusted access principles').[63]

Concerningly, there are various inconsistencies between and within state and federal data sharing legislation, including, for example, what constitutes 'personal information'.[64] These inconsistencies further limit the effective

No 1601, Faculty of Business and Law, University of the West of England, 2016) 21. See also Office of the National Data Commissioner, *Data Availability and Transparency Code 2022* (Consultation Paper, August 2022) 8 <https://www.datacommissioner.gov.au/sites/default/files/2022-08/Consultation%20Paper%20-%20DRAFT%20Data%20Code_1.pdf>, archived at <https://perma.cc/9XTE-NEQP>; Revised Explanatory Memorandum, Data Availability and Transparency Bill 2022 (Cth) 22 [122].

60 *NSW Data Sharing Act* (n 32) s 3; *SA Data Sharing Act* (n 32) s 4; *Vic Data Sharing Act* (n 32) s 1. In Queensland, the state government has released an '[i]nformation sharing authorising framework' for guiding government agencies seeking to establish and manage information sharing activities: Queensland Government Chief Information Office, *Information Sharing Authorising Framework: Comprehensive Guidance for Information Sharing* (Report, March 2018) 5–6 <https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-sharing-authorising-framework>.

61 *Vic Data Sharing Act* (n 32) ss 5, 15–18.

62 See, eg, *NSW Data Sharing Act* (n 32) ss 12–14; *SA Data Sharing Act* (n 32) ss 10–12. Cf *Vic Data Sharing Act* (n 32) pts 3–4.

63 See *SA Data Sharing Act* (n 32) s 7.

64 For example, 'personal information' under federal data sharing legislation and in some Australian states and territories is defined to include any information or opinion irrespective

regulation of data sharing agreements, as data sharing activities become subject to different and inconsistent laws.

Ultimately, data sharing legislation in Australia — both at the federal and state and territory levels — streamlines data flows between *particular* data sharing entities, often within jurisdictional boundaries, and leaves most of the concrete sharing arrangements to be negotiated and agreed upon by the data sharing entities themselves.

2 *Data Privacy Framework*

In Australia, data sharing legislation operates alongside privacy legislation. As the *DAT Act* specifies, data sharing activities must adhere to privacy legislation.[65] As privacy is not a constitutional right in Australia, privacy protections generally, and data privacy protection in particular, lie within the domains of both the Commonwealth and state and territory parliaments.[66] At the federal level, the main legislation governing data privacy elements of data sharing activities is the *Privacy Act*, which is currently undergoing a significant

of whether it is recorded in a material form or not: see, eg, *Cth DAT Act* (n 1) s 9 (definition of 'personal information'); *Cth Privacy Act* (n 2) s 6(1) (definition of 'personal information' para (b)); *NSW Data Sharing Act* (n 32) s 4(1) (definition of 'personal information'); *NSW Privacy Act* (n 2) s 4(1); *SA Data Sharing Act* (n 32) s 3(1) (definition of 'personal information'); *Vic Data Sharing Act* (n 32) s 3(1) (definition of 'personal information'); *Vic Privacy Act* (n 1) s 3 (definition of 'personal information'). However, in Tasmania, legislation concerning personal information restricts the definition of 'personal information' to information or opinion in recorded forms: *Right to Information Act 2009* (Tas) s 5(1) (definition of 'personal information') ('*Right to Information Act*'); *Tas Information Protection Act* (n 2) s 3 (definition of 'personal information'). The Northern Territory restricts personal information to information held by the government: *NT Information Act* (n 2) ss 4A(1)–(2). Additionally, in New South Wales and Tasmania, personal information does not include information about individuals who have been deceased for more than a certain amount of time (30 years and 25 years respectively): *NSW Data Sharing Act* (n 32) s 4(1) (definition of 'personal information'); *NSW Privacy Act* (n 2) s 4(3)(a); *Right to Information Act* (n 64) s 5(1) (definition of 'personal information'); *Tas Information Protection Act* (n 2) s 3 (definition of 'personal information'). In WA, however, identity information about a deceased person continues to be classified as 'personal': *WA Freedom of Information Act* (n 2) sch 1 cl 3(1).

65 *Cth DAT Act* (n 1) ss 13(1)(g), (i), 16E.

66 Morag Donaldson, 'Do Australians Have a Legal Right to Privacy?' (Research Note No 37, Parliamentary Library, Parliament of Australia, 14 March 2005) <https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/CBHF6/upload_binary/cbhf64.pdf;fileType%3Dapplication%2Fpdf>, archived at <https://perma.cc/565G-ZGCE>; Australian Law Reform Commission, *Review of Australian Privacy Law* (Discussion Paper No 72, September 2007) vol 1, 145–6 [2.2]–[2.4], 148 [2.13] <https://www.alrc.gov.au/wp-content/uploads/2019/08/DP72_full.pdf>, archived at <https://perma.cc/KBD7-535X> ('*Australian Privacy Law*').

review process and for which legislative reform is pending.[67] The *Privacy Act* applies to data sharing agreements between and within federal government entities and some private sector organisations to the extent that the shared data includes personal information.[68] Personal information is defined as information or an opinion about an identified individual (or an individual who is reasonably identifiable) whether it is true or not and irrespective of whether it is recorded in a material form or not.[69] Under the *Privacy Act*, the Australian Privacy Principle ('APP') 11 requires reasonable steps to protect personal information from, inter alia, unauthorised access and APPs 6–8 place explicit limitations on the intentional sharing of personal information.[70]

Similarly to the data sharing legislation, the APPs were designed from the standpoint of entities collecting and processing data, though they more clearly acknowledge data subjects' rights and interests.[71] The 'Consumer Data Right', which applies within particular sectors, grants consumers the right to access their data and to share it with accredited third parties of their choice.[72] Additional rights are also acknowledged and proposed to be implemented in the *Privacy Act Review* report.[73]

In addition to the federal legislation, most state and territory jurisdictions have enacted data privacy legislation that addresses state government and agency data holdings.[74] While Western Australia ('WA') and SA do not have specific laws, the *Freedom of Information Act 1992* (WA) provides some form

[67] *Cth Privacy Act* (n 2); *Australian Privacy Law* (n 66) 146 [2.5]; Mark Dreyfus, 'Privacy by Design Awards 2024' (Speech, Sydney, 2 May 2024) <https://ministers.ag.gov.au/media-centre/speeches/privacy-design-awards-2024-02-05-2024>; *Privacy Act Review* (n 17) 1. Proposal 29.3 of the Attorney-General's Department (Cth) report aims to mitigate this legislative fragmentation by establishing a Commonwealth, state and territory working group to harmonise privacy laws across Australia: at 16.

[68] *Cth Privacy Act* (n 2) ss 6(1) (definitions of 'agency', 'APP entity' and 'personal information'), 6C.

[69] Ibid s 6(1) (definition of 'personal information').

[70] *Cth Privacy Act* (n 2) sch 1 ('*Australian Privacy Principles*') cls 6–8, 11.1(b).

[71] For example, data subjects have the right to access their personal information and to seek its correction: ibid cls 5, 12–13. Cf at cls 3–4.

[72] *Competition and Consumer Act 2010* (Cth) ss 56AA–56AB; 'What Is the Consumer Data Right?', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right/>, archived at <https://perma.cc/JY2S-TMAS>.

[73] *Privacy Act Review* (n 17) 11–12, 166–93.

[74] See, eg, *ACT Privacy Act* (n 2) s 7; *NSW Privacy Act* (n 2) pt 2 div 1; *NT Information Act* (n 2) s 3; *Qld Privacy Act* (n 2) s 3; *Tas Information Protection Act* (n 2); *Vic Privacy Act* (n 1) s 1.

of privacy principles that safeguard personal information in WA;[75] the *Information Privacy Principles (IPPS) Instruction* issued by the Premier and Cabinet provides similar protection in SA.[76] In some jurisdictions, additional health-specific legislation further regulates the handling of *health data*.[77] The diverging approaches within and between jurisdictions makes it particularly challenging to streamline data flows and to guide data sharing activities that cross jurisdictions.[78]

To conclude, data sharing and data privacy (or data protection) legislation in Australia includes numerous, sometimes conflicting, instructions concerning data sharing activities that depend on a variety of factors and considerations. As a result, data sharing activities in Australia must adhere to different legal obligations depending on the relevant jurisdiction or jurisdictions, the types of the data sharing entities and the nature of the data being shared. Navigating this complicated legislation is a difficult task for data sharing entities and the conflicting terminologies and requirements hinder the development of a strong and effective organisational data sharing culture in Australia.

B *Regulatory Developments and Alternatives*

With data flows taking a more prominent role in the global economy, data protection and data privacy regimes are rapidly evolving.[79] Broadly speaking, there are two main approaches to data protection globally: a market-based approach, designed to protect consumers from market failures such as unfairness or deceptions, and a rights-based approach, which views data protection as a dignity and informational self-determination issue. While the

[75] See, eg, *WA Freedom of Information Act* (n 2) ss 10, 45.

[76] Department of the Premier and Cabinet (SA), *Information Privacy Principles (IPPS) Instruction* (PC 012, 1 July 2016) 3–8 <https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf>, archived at <https://perma.cc/ER5Q-EGG6>.

[77] See, eg, *Health Records (Privacy and Access) Act 1997* (ACT) s 3; *Health Records and Information Privacy Act 2002* (NSW) s 3; *Health Records Act 2001* (Vic) s 1; *Health Services Act 2016* (WA) pt 17.

[78] *Privacy Act Review* (n 17) 1, 302–3.

[79] João Marinotti, 'Data Types, Data Doubts & Data Trusts' (2022) 97 *New York University Law Review Online* 146, 162, 172.

first approach has been discussed in the United States ('US'),[80] the latter has been represented and advanced in the EU.[81] The cornerstone of the EU data protection regime is the *General Data Protection Regulation* ('*GDPR*').[82] Additionally, the EU data protection regime includes the recently enacted *Data Governance Act* ('*DGA*') which sets out to facilitate public sector data sharing and to strengthen confidence in data sharing mechanisms in order to increase data availability and reuse within the public sector.[83] These two arrangements have recently been complemented by the EU *Data Act*.[84] In addition to these regional laws, many EU countries legislate additional national laws that contain additional protections.[85] For example, in Germany, privacy is protected under the *German Constitution* and federal and state laws.[86] Despite various criticisms (including of its complex regulatory arrangements, the high costs of compliance, the vagueness of some of its requirements and its potential negative effects on competition and investment),[87] the *GDPR* is increasingly

[80] See, eg, Daniel J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53(6) *Stanford Law Review* 1393, 1445–55; Jessica Litman, 'Information Privacy/Information Property' (2000) 52(5) *Stanford Law Review* 1283, 1289–90.

[81] See Yvonne McDermott, 'Conceptualising the Right to Data Protection in an Era of Big Data' (2017) 4(1) *Big Data and Society*:1–7, 1–3; Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94(4) *New York University Law Review* 771, 773 ('Global Data Privacy').

[82] *GDPR* (n 5). See Schwartz, 'Global Data Privacy' (n 81) 771–3.

[83] *DGA* (n 5) recitals 3, 5, 19, art 1.

[84] *Data Act* (n 5). As opposed to the *GDPR* (n 5), which regulates the processing of personal data, the *Data Act* (n 5) is designed to regulate the stream of data generated by the 'Internet of Things' or other devices, regardless of the type of shared or streamed data (personal or not): at recital 14, arts 1(1)–(2); *GDPR* (n 5) arts 1–2.

[85] See, eg, Bart Custers et al, 'A Comparison of Data Protection Legislation and Policies across the EU' (2018) 34(2) *Computer Law and Security Review* 234, 235–6, 239–40, 243.

[86] See Hornung and Schnabel (n 33) 86; *German Constitution* (n 33) arts 1(1), 2(1) [tr Tomuschat et al (n 33) arts 1(1), 2(1)]; Bundesverfassungsgericht, 1 BvR 209/83 (n 33) 42–4 [tr 'Order of 15 December 1983' (n 33) [146]–[148]]; Bundesgerichtshof [German Federal Court of Justice], I ZR 211/53, 25 May 1954 reported in (1954) 13 BGHZ 334, 337–8; *Bundesdatenschutzgesetz* [Federal Data Protection Act] (Germany) 30 June 2017, BGBl I, 2017, 2097 [tr Federal Ministry of the Interior (Germany), 'Federal Data Protection Act', *Federal Ministry of Justice* (Web Document) <https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf>, archived at <https://perma.cc/ZR5X-79C4>]; *Hamburgisches Datenschutzgesetz* [Hamburg Data Protection Act] (Germany) 18 May 2018, HmbGVBl, 2018, 145.

[87] See, eg, Karen Yeung and Lee A Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16(1) *Regulation and Governance* 137, 138–43; Michal S Gal and Oshrit

recognised as the 'gold standard' for data protection,[88] shaping data protection laws not just within the EU but also globally.[89]

The Australian data protection and data privacy regime described above lies in between these two positions, with the recent *Privacy Act Review* proposals moving it closer to the EU approach.[90] These proposals to reform the *Privacy Act*, made by the Attorney-General's Department ('Department'), include major reforms to the Act's purposes, scope and obligations — many of which are inspired by the *GDPR*.[91] Some of the proposed changes would have a significant impact on the Act as a whole, including in relation to the definition of 'personal information' and the removal of both the small business exemption and, potentially, the employee records exemption.[92] Of particular relevance to the discussion here is a proposal to increase organisational accountability[93] as well as proposals to develop *GDPR*-like rights such as a right of erasure and a right to object to the collection, use or disclosure of personal information.[94] Further, there is a proposal that would require obtaining an individual's consent in order to 'trade' their personal information, although what would constitute 'trading' has not yet been specified.[95] There is also a proposal to enhance enforcement by introducing a direct right of action for data subjects (note that Australia has already increased potential penalties under the *Privacy Act*).[96] The Australian Government has agreed or agreed in principle with many of the

Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) *Journal of Competition Law and Economics* 349, 351, 366–77.

88 Michael L Rustad and Thomas H Koenig, 'Towards a Global Data Privacy Standard' (2019) 71(2) *Florida Law Review* 365, 366, 431–48, 453.

89 Ibid 449, 453; Schwartz, 'Global Data Privacy' (n 81) 773, 777–8.

90 Subject to certain conditions, the *Cth Privacy Act* (n 2) recognises the interests of businesses to collect, use and disclose individuals' data: see, eg, *Australian Privacy Principles* (n 70) cls 3, 6. At the same time, that legislation also provides certain rights to individuals — namely, the rights to access and correct personal information: at cls 12–13. See also *Privacy Act Review* (n 17) 3, 11–12, 166–93.

91 *Privacy Act Review* (n 17) 1–16, 166–93; *GDPR* (n 5) arts 12–23.

92 *Privacy Act Review* (n 17) 5–7, 23–9, 56–71. See also Paterson and McDonagh (n 3) 9–10, 15–25. Cf *Cth Privacy Act* (n 2) ss 6(1) (definitions of 'personal information' and 'employee record'), 6C(1), 6D, 7B(3).

93 *Privacy Act Review* (n 17) 10, 140–5.

94 Ibid 11–12, 172–6. Cf *GDPR* (n 5) arts 17, 21.

95 *Privacy Act Review* (n 17) 12, 210–11, 214.

96 Ibid 15, 272–9; *Cth Privacy Act* (n 2) s 13G, later amended by *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) sch 1 item 14.

Department's proposals but draft legislation is yet to be released.[97] In this Part, we briefly outline a sample of possibilities that might resolve some of the concerns we raise about data governance in the context of data sharing.

1 *Data Subjects' Rights*

As a part of reviewing the *Privacy Act*, the Australian Government agreed in principle that individuals should have greater control over their personal information through such rights as a right to erasure or de-identification and a right to challenge an entity on its data handling practices (subject to exceptions).[98] However, the Australian Government also acknowledged that such rights could be burdensome and that the issue thus required 'further consideration'.[99] Including some data subjects' rights in the Australian data privacy regime would improve the regime's protection of personal information and develop a stronger data rights culture in Australia, bringing the Australian *Privacy Act* closer to the EU's *GDPR*.[100] However, some differences would remain. Fundamentally, as the rights to privacy and data protection are included in the *Charter of Fundamental Rights of the European Union* as well as in the *Convention for the Protection of Human Rights and Fundamental Freedoms*,[101] one of the *GDPR*'s core features and main policy objectives has been to reflect these rights through detailed restrictions on data practices.[102] The proposed *Privacy Act* reforms would incorporate some of the specific data rights without making a similar connection to fundamental human rights (thus leaving some concrete and potential gaps in the protection afforded to data subjects).[103]

[97] Australian Government, *Government Response: Privacy Act Review Report* (Report, 2023) 2, 21–38 <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>, archived at <https://perma.cc/9R43-T2EG> ('*Government Response*'); *Privacy Act Review* (n 17) 5–16.

[98] *Government Response* (n 97) 18, 30–1.

[99] Ibid 18.

[100] *Privacy Act Review* (n 17) 3, 166, discussing *Cth Privacy Act* (n 2); *GDPR* (n 5) arts 12–23.

[101] *Charter of Fundamental Rights of the European Union* [2016] OJ C 202/389, arts 7–8; *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 8.

[102] *GDPR* (n 5) recitals 1, 73, arts 12–23.

[103] See *Privacy Act Review* (n 17) 18–22.

2 *Allocation of Data Protection Responsibilities*

Another element in the proposed *Privacy Act Review* includes a distinction between the 'controllers' and the 'processors' of personal data.[104] This distinction alludes to the *GDPR*'s framework, which details data processing responsibilities and dictates specific codes of conduct for data controllers and for data processors, including an accountability principle that holds the data controller accountable for actions conducted by the data processor and responsible for demonstrating compliance with the data processing requirements.[105] By contrast, the distinction between controllers and processors in the *Privacy Act Review* is framed in terms of the need to clarify obligations and 'reduce the compliance burden for … processors' rather than in terms of the need to ensure accountability of controllers.[106] It seems unlikely that Australia will go as far as the *GDPR* in essentially requiring controllers to regulate data processors.[107]

3 *Specific Requirements for Data Processing Agreements*

Some proposals included in the *Privacy Act Review*, with which the government agrees in principle, could lead to improvements in data sharing agreements.[108] Two such examples are the proposal to introduce a 'fair and reasonable' test[109] and a requirement for all entities to undertake a 'Privacy Impact Assessment' prior to high privacy risk activities.[110] While these are significant and welcomed improvements, these proposals do not go as far as some of the requirements included in the *GDPR* regime, which require that data processing agreements provide sufficient guarantees to implement appropriate technical and organisational measures to ensure compliance.[111] This focus on technical

[104] Ibid 4, 230–3.

[105] See, eg, *GDPR* (n 5) arts 5, 24, 28. 'Data controllers' are entities who determine the purposes and means of data processing, while 'data processors' are entities who process data on behalf of a data controller: at arts 4(7)–(8). Finally, 'data recipients' are entities to which 'personal data are disclosed': at art 4(9).

[106] *Government Response* (n 97) 15. See also *Privacy Act Review* (n 17) 231–3.

[107] Cf *GDPR* (n 5) arts 5, 29.

[108] See *Government Response* (n 97) 21–38; *Privacy Act Review* (n 17) 5–16.

[109] *Government Response* (n 97) 8. See also *Privacy Act Review* (n 17) 112–21.

[110] *Government Response* (n 97) 10. See also *Privacy Act Review* (n 17) 124–7.

[111] *GDPR* (n 5) art 28. Consistently with the *GDPR*'s broad definitions for data processing, a data processing agreement governs the relationship between a data controller and a data processor,

measures and capabilities, which is not currently being considered in the *Privacy Act Review*, is significant, as it could overcome the mismatch between legal requirements and actual practices.[112]

To conclude, depending on which proposals are adopted, there is potential to enhance Australia's data privacy regime, bringing it closer to the EU approach.[113] However, the prevalence of the *GDPR* regime and its global impact lie not only in the regime's detailed requirements and mechanisms but also in the recognition of data privacy as a fundamental right within the EU and of the regime's extraterritorial impact.[114] From this perspective, Australia's soon-to-be reformed *Privacy Act* will still retain gaps in data protection, mainly due to its potentially limited jurisdictional scope and lack of grounding in a human rights framework.[115]

III Governing Data Sharing through Adapting Private Law Frameworks

This Part explores how private law frameworks might be adapted to provide for data governance in the context of data sharing arrangements. Some of these ideas hinge on the question of whether there is identifiable property.[116] In particular, when the law recognises a 'thing' as a potential object of property rights, there are doctrinal categories through which different kinds of sharing can occur.[117] Each of these categories comes with its own rights, duties, powers

specifying how personal data is processed and protected when outsourcing processing activities: at arts 4(2), (7)–(8), 5, 28.

112 See *Privacy Act Review* (n 17) 5–16; Christopher Millard and Dimitra Kamarinou, 'Article 28: Processor' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 599, 605.

113 There are other features of the *GDPR* (n 5) that are not included in the existing recommendations, such as the right to receive data (upon request) in a portable format: see, eg, at art 20; *Privacy Act Review* (n 17) 166.

114 Schwartz, 'Global Data Privacy' (n 81) 772–3, 776–8; *GDPR* (n 5) recitals 1, 22, arts 1(2), 3.

115 See above nn 67, 74–8 and accompanying text. See also *Cth Privacy Act* (n 2) s 5B; *Privacy Act Review* (n 17) 234–7; *Government Response* (n 97) 16, 34.

116 See below Part III(A).

117 See Australian Law Reform Commission, *Traditional Rights and Freedoms: Encroachments by Commonwealth Laws* (Final Report No 129, December 2015) 463 [18.17] <https://www.alrc.gov.au/wp-content/uploads/2019/08/alrc_129_final_report_.pdf>, archived at <https://perma.cc/K694-HXYV>; *Yanner v Eaton* (1999) 201 CLR 351, 366–7 [19]–[20] (Gleeson CJ, Gaudron, Kirby and Hayne JJ), 388 [85] (Gummow J).

and liabilities both *between* the sharing parties but also with respect to third parties.[118] Thus, parties with proprietary rights can 'share' through mechanisms such as co-ownership, express trusts, bailment (for chattels) and leases (for land).[119] The legal framework for sharing is based on the objective intention of the parties (eg an intention to create a trust).[120] These mechanisms become available if 'data', or a right related to 'data', is recognised as a 'thing'; consequently, this Part considers whether private law mechanisms could be adapted to sharing arrangements involving data in a way that improves data governance. It explores the propertisation of data, data 'trusts' and information 'fiduciaries'.

A *Data as Property in Australia*

In Australia, information is not property.[121] Decisions in contexts including the interpretation of taxation legislation, access to medical records, knowing assistance and receipt, and the proceeds of crime have refused to treat information as proprietary.[122] For example, a payment made for information is

[118] Determann (n 2) 8–9; Brendan Edgeworth et al, *Sackville & Neave: Australian Property Law* (LexisNexis, 11th ed, 2021) 333–4 [4.155]–[4.157].

[119] See, eg, *Wright v Gibbons* (1949) 78 CLR 313, 330 (Dixon J); Geraint Thomas and Alastair Hudson, *The Law of Trusts* (Oxford University Press, 2nd ed, 2010) 1495 [58.04], quoted in *Byrnes v Kendle* (2011) 243 CLR 253, 263 [17] (French CJ) ('*Byrnes*'); *Penfolds Wines Pty Ltd v Elliott* (1946) 74 CLR 204, 214, 216 (Latham CJ), 224 (Dixon J), 241–2 (Williams J); *Radaich v Smith* (1959) 101 CLR 209, 215 (McTiernan J, Dixon CJ agreeing at 213), 217 (Taylor J, Dixon CJ agreeing at 213), 221–2 (Windeyer J, Dixon CJ agreeing at 213); Edgeworth et al (n 118) 87–8 [2.18]–[2.19], 262–3 [4.82], 512–16 [6.2E]–[6.6E], 616 [8.8].

[120] *Byrnes* (n 119) 261–4 [14]–[18] (French CJ), 273–6 [53]–[60] (Gummow and Hayne JJ), 284–6 [98]–[101] (Heydon and Crennan JJ). See also Edgeworth et al (n 118) 87–8 [2.18], 617–18 [8.11]–[8.14].

[121] See, eg, *Moorgate Tobacco Co Ltd v Philip Morris Ltd [No 2]* (1984) 156 CLR 414, 441, where Deane J held that '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 Federal Commissioner of Taxation* (1971) 125 CLR 418, 425, where Gibbs J held that '[n]either knowledge nor information is property in a strictly legal sense'; *Federal Commissioner of Taxation v Sherritt Gordon Mines Ltd* (1977) 137 CLR 612, 630, where Jacobs J held that 'the possessor of the "know-how" has no right in it against the world'; *Pancontinental Mining Ltd v Commissioner of Stamp Duties* [1989] 1 Qd R 310, 311, where de Jersey J held that 'the ordinary meaning of the word [property] does not encompass information'.

[122] See, eg, *Federal Commissioner of Taxation v United Aircraft Corporation* (1943) 68 CLR 525, 533–6 (Latham CJ) ('*United Aircraft*'); *Breen v Williams* (1996) 186 CLR 71, 77, 80–1

not derived from 'property' and communicating information would not constitute a transfer of property.[123] Similar logic also applies to data and digital files; this logic can also be seen in other common law jurisdictions.[124] Not recognising data as a 'thing' to which property rights attach is consistent with the Productivity Commission's findings in its *Data Availability and Use* report.[125] Thus, despite the fact that data is often treated as a market commodity, where data subjects disclose information about themselves in exchange for goods and services there is no transfer of property from the data subject to the data collector.[126] Although journalists are inclined to ask who 'owns' data,[127] organisations sometimes use the term 'ownership' to describe practical

(Brennan CJ), 88–90 (Dawson and Toohey JJ), 111–12 (Gaudron and McHugh JJ), 128–9 (Gummow J) ('*Breen*'); *Consul Development Pty Ltd v DPC Estates Pty Ltd* (1975) 132 CLR 373, 405, 414 (Stephen J, Barwick CJ agreeing at 376–7, McTiernan J dissenting at 386); *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* (2007) 230 CLR 89, 143–4 [117]–[119] (Gleeson CJ, Gummow, Callinan, Heydon and Crennan JJ) ('*Farah Constructions*'); *Denlay v Federal Commissioner of Taxation* (2011) 193 FCR 412, 431–2 [68]–[74] (Keane CJ, Dowsett and Reeves JJ).

123 *United Aircraft* (n 122) 534 (Latham CJ).

124 See Johan David Michels and Christopher Millard, 'Mind the Gap: The Status of Digital Files under Property Law' (Research Paper No 317/2019, School of Law, Queen Mary University of London, 2019) 7–11 <https://ssrn.com/abstract=3387400>, archived at <https://perma.cc/5A96-MCQZ>; Aaron Perzanowski and Jason Schultz, *The End of Ownership: Personal Property in the Digital Economy* (MIT Press, 2016) 45–8, 55; Determann (n 2) 11–26.

125 Productivity Commission, *Data Availability* (n 3) 191, 196–7.

126 See Simon G Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in Philip E Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press, 1997) 143, 160–1; Paul M Schwartz, 'Property, Privacy, and Personal Data' (2004) 117(7) *Harvard Law Review* 2056, 2057; Marinotti (n 79) 147–8.

127 See, eg, Nigel Shadbolt and Roger Hampson, 'Who Should Hold the Keys to Our Data?', *The Guardian* (online, 29 April 2019) <https://www.theguardian.com/commentisfree/2018/apr/29/in-charge-our-own-data-personal-information-facebook-scandal>, archived at <https://perma.cc/5S5V-6F3F>; Alex Hern, 'Sir Tim Berners-Lee Speaks Out on Data Ownership', *The Guardian* (online, 8 October 2014) <https://www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership>, archived at <https://perma.cc/6ATW-Z6CU>.

control[128] and organisations exercise similar practical control over data as they do over property,[129] data is not in fact 'owned'.[130]

The reason why data is not a 'thing' in property law derives from its non-rivalrous nature.[131] For most 'things', including intangible assets such as shares, two people cannot possess or own the same thing without encountering a need to share; for example, when two people simultaneously own the same plot of land, they must share that plot of land as co-owners, co-beneficiaries or the like.[132] However, one entity can transfer a copy of data to a second entity without losing the technical ability to control, use and further distribute that data.[133] Thus, data has a 'magic pudding' problem in that multiple entities can benefit from the same data (or copies thereof) without interfering with each other's use.[134]

Despite the state of existing law, one could, through statutory intervention, deem data to be a potential object of property rights.[135] The arguments for propertising data have focused on the national interest,[136] the importance of

[128] See, eg, Global Initiative on Ethics of Autonomous and Intelligent Systems, Institute of Electrical and Electronics Engineers, *Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems* (Report, 2017) 237–9 <https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf>, archived at <https://perma.cc/X23Z-8RFW>. Cf Bennett Moses (n 53) 619–20, 624–5.

[129] Gianclaudio Malgieri, 'Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data' [2016] (4) *Privacy in Germany* 133, 134 ('Property and (Intellectual) Ownership').

[130] See above n 121 and accompanying text. See also Bennett Moses (n 53) 627–8.

[131] See Johan David Michels and Christopher Millard, 'The New Things: Property Rights in Digital Files?' (2022) 81(2) *Cambridge Law Journal* 323, 327–8, 335 ('The New Things'). But see Nadezhda Purtova, 'Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence' in Serge Gutwirth et al (eds), *Computers, Privacy and Data Protection: An Element of Choice* (Springer, 2011) 39, 56–8 ('Property in Personal Data').

[132] David Milman, *The Company Share: Legal Regulation and Public Policy* (Edward Elgar, 2018) 72; 'Joint Ownership of Shares', *Australian Taxation Office* (Web Page, 4 July 2023) <https://www.ato.gov.au/forms-and-instructions/you-and-your-shares-2023/joint-ownership-of-shares>, archived at <https://perma.cc/58ZH-BRBE>; Edgeworth et al (n 118) 55–6 [1.74], 511 [6.1].

[133] Michels and Millard, 'The New Things' (n 131) 335–6.

[134] Ibid. See Norman Lindsay, *The Magic Pudding: Being the Adventures of Bunyip Bluegum* (Angus & Robertson, 1918) 23.

[135] See Determann (n 2) 9–11; Bennett Moses (n 53) 630.

[136] See Evgeny Morozov, 'To Tackle Google's Power, Regulators Have to Go after Its Ownership of Data', *The Guardian* (online, 2 July 2017) <http://www.theguardian.com/

data and the way it is handled for human rights or civil liberties (particularly the right to privacy),[137] competition policy,[138] data subjects securing more control,[139] efficiency benefits (between data subjects and organisations),[140] ways to address market failures,[141] legal clarity and good governance[142] and ways to fill gaps in the availability of remedies;[143] these arguments have also been influenced by political, rhetoric or legal factors in particular jurisdictions.[144] These benefits are linked not only to the possibility of different sets of sharing rules between parties, such as those associated with bailment,[145] but also to the fact that actions and remedies associated with proprietary torts would be available.[146] An individual with *property* rights over data, for example, could sue in conversion if an entity acted inconsistently with those rights.[147] The

technology/2017/jul/01/google-european-commission-fine-search-engines>, archived at <https://perma.cc/2E7D-Z4Y7>; Determann (n 2) 9–11.

137 See Perzanowski and Schultz (n 124) 192. But see Pamela Samuelson, 'Privacy as Intellectual Property?' (2000) 52(5) *Stanford Law Review* 1125, 1128, 1142–3.

138 Morozov (n 136).

139 Lawrence Lessig, *Code: And Other Laws of Cyberspace* (Basic Books, 1999) 159–61; Patricia Mell, 'Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness' (1996) 11(1) *Berkeley Technology Law Journal* 1, 46, 74–81; Malgieri, 'Property and (Intellectual) Ownership' (n 129) 135–6; Vera Bergelson, 'It's Personal but Is It Mine? Toward Property Rights in Personal Information' (2003) 37(2) *University of California, Davis Law Review* 379, 383, 400–3.

140 See Kenneth C Laudon, 'Markets and Privacy' (1996) 39(9) *Communications of the ACM* 92, 93, 99–101; Charles I Jones and Christopher Tonetti, 'Nonrivalry and the Economics of Data' (2020) 110(9) *American Economic Review* 2819, 2819–20, 2853–5.

141 See Florent Thouvenin, Rolf H Weber and Alfred Früh, 'Data Ownership: Taking Stock and Mapping the Issues' in Matthias Dehmer and Frank Emmert-Streib (eds), *Frontiers in Data Science* (CRC Press, 2018) 111, 114–18. Ultimately, however, Thouvenin, Weber and Früh find against creating a data ownership right, instead preferring specific regulation: at 119–20, 129–32, 136–7.

142 See Telecom Regulatory Authority of India, *Privacy, Security and Ownership of the Data in the Telecom Sector* (Consultation Paper, 9 August 2017) 6–7 [2.4]–[2.5] <https://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf>, archived at <https://perma.cc/93G7-ULXD>; Purtova, 'Property in Personal Data' (n 131) 56–8.

143 Michels and Millard, 'The New Things' (n 131) 344–7.

144 Nadezhda Purtova, 'Property Rights in Personal Data: Learning from the American Discourse' (2009) 25(6) *Computer Law and Security Review* 507, 508–9, 515–19 ('Learning from the American Discourse'); Lawrence Lessig, 'Privacy as Property' (2002) 69(1) *Social Research* 247, 247, 254–6.

145 See above nn 118–19 and accompanying text.

146 Michels and Millard, 'The New Things' (n 131) 344, 347.

147 Ibid.

question of who would own the data once it was propertised is contentious, but suggested owners include a 'national data fund' co-owned by all citizens, individual data subjects, the entity engaging in an activity related to the data, the entity with de facto control of the data and the entity best able to make economic use of the data.[148] There are also questions about what the nature of the property would be: the data as such or the digital file in the logical layer of software applications (eg a DOCX or a PDF file).[149]

A related idea to the direct propertisation of data is to draw on intellectual property law and create a statutory right similar to the EU's sui generis protection of 'databases' in *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases*.[150] This directive protects collections 'arranged in a systematic or methodical way and individually accessible by electronic or other means'.[151] It does *not* protect individual elements in the database.[152] The database right thus protects investment in database creation but does not provide a useful mechanism for data governance since the right is not breached by the lawful extraction and use of the data (unless the extraction is of a substantial part of the data).[153] A similar point applies to copyright in arrangements of data where a copyright exists.[154]

One variable evident in discussions about propertising data is the circumstances under which it could be freely alienated. In some proposals, data subjects would have the power to sell their data (and thus share in some of its economic value), while in others this ability would be restricted.[155] There are also more complex proposals for specific alienability structures such as requiring affirmative consent from a data subject for additional uses or transfers

[148] See Morozov (n 136); Václav Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34(5) *Computer Law and Security Review* 1039, 1041, 1044–9; Bergelson (n 139) 419–36.

[149] Michels and Millard, 'The New Things' (n 131) 343–54; Bennett Moses (n 53) 631; Determann (n 2) 13–14.

[150] *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases* [1996] OJ L 77/20, arts 1, 3, 7.

[151] Ibid art 1(2).

[152] Ibid art 3(2).

[153] Ibid arts 7(1), 8(1).

[154] Ibid arts 3, 7(4).

[155] For a summary of some of these proposals, see Schwartz, 'Property, Privacy, and Personal Data' (n 126) 2090–4.

beyond initial collection (thus preventing a data subject from 'selling' unrestricted eternal rights to their personal information).[156]

Nadezhda Purtova offers a comprehensive argument as to why data should be treated as an object of property rights.[157] In Purtova's scholarship, propertisation of data (in the sense of recognising in rem rights over data) can enhance informational self-determination and usefully supplement data protection laws.[158] In Purtova's view, the information industry already has a de facto claim to exclusive rights in personal data and so the only question to consider is not *whether* data is property but instead *who* owns it.[159] In our view, Purtova is correct to say that some entities exercise de facto control over data. De facto control arises through a variety of means — for example, data subjects can in most circumstances choose what information to share[160] and the entities possessing physical media on which data is stored are protected both practically and through some computer crime statutes that make it an offence to access that data without authorisation.[161] This is still different to a property right in data itself as the nature of available remedies and available ownership structures are distinct.[162] Property ownership structures cannot be applied; therefore, data sharing contracts (constrained by law but not by *numerus clausus*)[163] remain a primary mechanism for agreeing to alter rights, duties, powers and liabilities with respect to data.[164] However, we agree with Purtova that the question of

156 Ibid 2097–8.

157 Purtova, 'Property in Personal Data' (n 131) 49–62; Purtova, 'Learning from the American Discourse' (n 144) 508, 514–19; Nadezhda Purtova, 'The Illusion of Personal Data as No One's Property' (2015) 7(1) *Law, Innovation and Technology* 83, 100–11 ('The Illusion of Personal Data'); Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Wolters Kluwer, 2012) 245–61 ('*A European Perspective*').

158 Purtova, *A European Perspective* (n 157) 70, 246–56, 269–70.

159 Purtova, 'The Illusion of Personal Data' (n 157) 104–11.

160 However, it should be noted that a failure to share may affect data subjects' ability to access certain services: ibid 105–6.

161 Determann (n 2) 13–14; *Criminal Code Act 1995* (Cth) s 478.1. For similar (though not necessarily equivalent) provisions, see *Criminal Code 2002* (ACT) s 415; *Crimes Act 1900* (NSW) s 308C; *Criminal Code Act 1983* (NT) s 276B; *Criminal Code Act 1899* (Qld) s 408E; *Criminal Law Consolidation Act 1935* (SA) s 86E; *Criminal Code Act 1924* (Tas) s 257D; *Crimes Act 1958* (Vic) s 247B; *Criminal Code Act Compilation Act 1913* (WA) s 440A.

162 See above nn 121–47 and accompanying text. See also Determann (n 2) 13–14.

163 Purtova, *A European Perspective* (n 157) 78.

164 Kevin E Davis and Florencia Marotta-Wurgler, 'Contracting for Personal Data' (2019) 94(4) *New York University Law Review* 662, 663. See below Part IV.

whether data *ought to become* property is separate from the question of whether it is already property.[165]

While some have argued in support of propertising data, there are also arguments against propertisation. The Productivity Commission has argued that consumers should be given *rights* over their data but not *ownership*.[166] The Productivity Commission gave two main reasons for this view. First, data ownership would be complex because of its overlap with copyright law and the competing interests in data (eg among people in a photograph); data ownership would thereby complicate desirable data use.[167] Secondly, consumer rights over their data ought to be inalienable.[168] The Max Planck Institute for Innovation and Competition also opposed granting property-like rights in data, citing harm to the economy and legal uncertainty.[169] A number of scholars have also expressed concern about the idea of propertisation, particularly if it includes commodification.[170] One can imagine strange scenarios where individuals are forced to sell their data to maximise the assets that they have available to a trustee in bankruptcy.[171]

To date, there have been few local voices in favour of propertising data in Australia, and law reform processes are following the Productivity Commission's lead in disfavouring property rights for alternative frameworks.[172] Internationally, however, there is more interest in identifying 'digital assets' that could be made objects of property rights. The British Law Reform Commission has looked at the issue of property rights in digital assets in England and Wales, recommending statutory confirmation of a category of property that is neither *choses in action* nor *choses in possession* in order to

165 Purtova, *A European Perspective* (n 157) 1–2, 60–1.

166 Productivity Commission, *Data Availability* (n 3) 196–7.

167 Ibid.

168 Ibid.

169 Josef Drexl et al, 'Data Ownership and Access to Data: Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate' (Research Paper No 16-10, Max Planck Institute for Innovation and Competition, 16 August 2016) 2–3 [4]–[8] <https://papers.ssrn.com/abstract=2833165>, archived at <https://perma.cc/4YEN-J6WS>.

170 See, eg, Solove (n 80) 1445–55; Litman (n 80) 1296–301.

171 See Solove (n 80) 1430, 1452; *Mannigel v Aitken* (1983) 77 FLR 406, 408 (Smithers J).

172 See, eg, Productivity Commission, *Data Availability* (n 3) 196–7; *Privacy Act Review* (n 17) 166–79.

accommodate digital assets such as crypto-tokens.[173] This recommendation would not necessarily change the underlying position regarding what kinds of 'things' can be objects of property rights, and the reports acknowledge that pure information has long been held not to be an object of property rights.[174] The International Institute for the Unification of Private Law's *Principles on Digital Assets and Private Law* ('*Principles*') state that 'digital assets' (ie electronic records capable of being subject to control) can be the object of property rights.[175] However, the information content would be a separate matter from this 'digital asset',[176] so while a password-protected file could be a digital asset, personal information contained in that file gains no new status.[177] Thus, 'data' as such is not property; only files that require some kind of mechanism (such as a password) to be accessed would be property, because such files would be in the exclusive control of their owner.[178] Even there, as the *Principles* acknowledge, this property right has little practical effect outside of domains such as cryptocurrency.[179] This makes sense — the magic pudding problem and the resulting lack of exclusivity make data a poor fit with property doctrine.[180] Any propertisation of data would necessarily involve extensive adaptations of property law.

[173] Law Commission (UK), *Digital Assets as Personal Property: Supplemental Report and Draft Bill* (Report No 416, 29 July 2024) 21–2 [2.54]–[2.58], 28–9 [2.83]–[2.88] <https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/07/Digital-assets-as-personal-property-supplemental-report-and-draft-Bill-web-version.pdf>, archived at <https://perma.cc/DEN4-TUJG>.

[174] Ibid 12–13 [2.25]; Law Commission (UK), *Digital Assets* (Final Report No 412, 27 June 2023) 65–71 [4.27]–[4.47] <https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2023/06/Final-digital-assets-report-FOR-WEBSITE-2.pdf>, archived at <https://perma.cc/7EJM-MQA2>.

[175] *Principles on Digital Assets and Private Law*, UNIDROIT Doc CD (102) 6 (April 2023, adopted 10 May 2023) (Adoption of Draft UNIDROIT Instruments) 16 principle 2(2), 23 principle 3(1), 38 principle 6(1).

[176] Ibid 19 [2.14]–[2.15].

[177] Ibid 19 [2.17].

[178] Ibid.

[179] Ibid 18 [2.8]–[2.9], 19 [2.17].

[180] See above n 134 and accompanying text. See also Michels and Millard, 'The New Things' (n 131) 328.

B *Alternatives to Propertisation: Data Trusts and Information Fiduciaries*

1 *Data Trusts*

In Europe and the US, 'data trust' solutions to the data governance challenge have been presented.[181] While not all of these solutions involve 'trusts' in the private law sense,[182] the focus in this Part is on those solutions that do. Express trusts are well established in equity; rules govern their creation as well as the rights, duties, powers and liabilities that result from their creation.[183]

There are examples of data trusts in Europe and the US that create new entities with a public mission such as entities that collate health data for research purposes and those that provide data governance options for data subjects.[184] These *new* entities are created specifically for collective management of data subjects' rights.[185] The trust can be set up differently, depending on the goals of the data trust project.[186]

[181] See, eg, Aapti Institute and Open Data Institute, *Enabling Data Sharing for Social Benefit through Data Trusts: An Interim Report for the 2021 GPAI Paris Summit* (Report, 2021) 37 <https://gpai.ai/projects/data-governance/data-trusts/enabling-data-sharing-for-social-benefit-data-trusts-interim-report.pdf>, archived at <https://perma.cc/VZ9J-76XD>; 'About', *Data Trusts Initiative* (Web Page) <https://datatrusts.uk/about>, archived at <https://perma.cc/3G96-8U5M>; 'The Light Collective Data Trust', *MIT Solve* (Web Page, 2024) <https://solve.mit.edu/challenges/horizonprize/solutions/50295> ('Light Collective'). See generally Sylvie Delacroix and Neil D Lawrence, 'Bottom-Up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance' (2019) 9(4) *International Data Privacy Law* 236, 239–41, 248–50.

[182] See, eg, Dame Wendy Hall and Jérôme Pesenti, *Growing the Artificial Intelligence Industry in the UK* (Report, 2017) 46 <https://assets.publishing.service.gov.uk/media/5a824465e5274a2e87dc2079/Growing_the_artificial_intelligence_industry_in_the_UK.pdf>, archived at <https://perma.cc/9E54-Y42Y>.

[183] See generally MW Bryan, VJ Vann and S Barkehall Thomas, *Equity & Trusts in Australia* (Cambridge University Press, 3rd ed, 2023) 211–13.

[184] See, eg, 'Light Collective' (n 181); 'Pilot Projects GPData', *Data Trusts Initiative* (Web Page) <https://datatrusts.uk/pilot-projects-gpdata>, archived at <https://perma.cc/69JD-Q3JP>.

[185] Delacroix and Lawrence (n 181) 242–3. See, eg, 'Light Collective' (n 181); 'Brixham Data Trust', *Data Trusts Initiative* (Web Page) <https://datatrusts.uk/pilot-brixham>, archived at <https://perma.cc/CRQ3-P8AX>.

[186] Delacroix and Lawrence (n 181) 240–1; Ada Lovelace Institute and UK AI Council, *Exploring Legal Mechanisms for Data Stewardship* (Final Report, March 2021) 34 <https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Legal-mechanisms-for-data-stewardship_report_Ada_AI-Council-2.pdf>, archived at <https://perma.cc/UXH6-H2XX>; *Data Trusts* (n 23) 14–19; Bryan, Vann and Barkehall Thomas (n 183) 211–13.

Trust law has a fairly flexible conception of 'property', extending it to any recognised legal entitlement.[187] For example, a 'trade secret' (comprising a right corresponding to a duty to keep certain information secret) can be held on trust as can patent rights.[188] However, since there are no legally recognised rights in 'data' (as there would be if data were property), data itself cannot be the subject matter of a trust (at least under Australian law).[189] If data trusts were to be deployed in Australia for a data governance purpose, this would need to be done by choosing trust property adjacent to the data itself. For example:

1 People might share data with an entity on the basis that the entity will only share the data with others who promise to keep it secret. The entity then would declare that it holds the benefit of such promises on trust for the data subjects. The trust property would be the right corresponding to the obligation to keep the secret; or

2 The statutory rights that data subjects have under data protection statutes (in the literature, this is the *GDPR*; in Australia, it would be privacy legislation) might be assigned to an entity that holds those rights on trust for the data subject.[190]

Each of these scenarios has its own challenges when considered in the Australian legal context and some have been questioned in the other jurisdictions in which they have been proposed.[191]

The first scenario can work from a doctrinal perspective. There, the trust property would be the right corresponding to an obligation, or obligations, of

[187] See Bryan, Vann and Barkehall Thomas (n 183) 134; James Edelman, 'Two Fundamental Questions for the Law of Trusts' (2013) 129 (January) *Law Quarterly Review* 66, 66.

[188] See *Farah Constructions* (n 122) 143–4 [118] (Gleeson CJ, Gummow, Callinan, Heydon and Crennan JJ); Bryan, Vann and Barkehall Thomas (n 183) 194 [12.1]; Marinotti (n 79) 157; *Neobev Pty Ltd v Bacchus Distillery Pty Ltd (admins apptd) [No 3]* (2014) 104 IPR 249, 267 [114] (Besanko J).

[189] See above Part III(A).

[190] Delacroix and Lawrence (n 181) 244–6; Ada Lovelace Institute and UK AI Council (n 186) 28–9, 37; Data Trusts Initiative, 'Data Trusts: From Theory to Practice' (Working Paper No 1, Data Trusts Initiative, 26 November 2020) 4–5 <https://static1.squarespace.com/static/5e3b09f0b754a35dcb4111ce/t/5fdb21f9537b3a6ff2315429/1608196603713/Working+Paper+1+-+data+trusts+-+from+theory+to+practice.pdf>, archived at <https://perma.cc/Y2BJ-435G>. See also *GDPR* (n 5); *Cth Privacy Act* (n 2); *ACT Privacy Act* (n 2); *NSW Privacy Act* (n 2); *NT Information Act* (n 2); *Qld Privacy Act* (n 2); *Tas Information Protection Act* (n 2); *Vic Privacy Act* (n 1).

[191] See Marinotti (n 79) 150, 153, 158–60.

confidence.[192] It has been proposed in the EU context that personal data ought to be treated as trade secrets (following the understanding of trade secrets in US law).[193] In Australia, this scenario would produce a right to have the information kept confidential; this right could be held on trust.[194] However, there are practical problems with using this mechanism for the purposes of data governance. The right would only be enforceable against parties who owe an obligation of confidence; it would not be enforceable against entities who gain access to the same data independently and it would only be invocable where there is an enforceable contractual or equitable obligation to keep the information confidential.[195] Therefore, in this scenario, the terms of the data sharing agreement between the trustee and the other entity would be crucial. The primary benefit to the data subjects would be the right to share in pecuniary damages or compensation for breach of those contracts.[196]

The second scenario is unlikely to work in Australia. In particular, it is not clear that Australian data privacy legislation would permit data subjects' statutory rights to be settled on trust. The primary 'right' is to complain if information is used without the consent of *the individual*; there is no mechanism in the *Privacy Act* for appointing an agent or settling this right on trust.[197] The same problem arises in the context of the right to access information being held on trust.[198]

[192] See *Farah Constructions* (n 122) 143–4 [118] (Gleeson CJ, Gummow, Callinan, Heydon and Crennan JJ); *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* (1990) 22 FCR 73, 87 (Gummow J) ('*Smith Kline*').

[193] Gianclaudio Malgieri, '"Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?' (2016) 20(5) *Journal of Internet Law* 3, 3, 10–11.

[194] *Smith Kline* (n 192) 120–1 (Gummow J); *Farah Constructions* (n 122) 143–4 [118] (Gleeson CJ, Gummow, Callinan, Heydon and Crennan JJ).

[195] *Smith Kline* (n 192) 87, 121 (Gummow J); Bryan, Vann and Barkehall Thomas (n 183) 197–8, 204–5. See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 1, 565–6 [15.125]–[15.128] <https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf>, archived at <https://perma.cc/DA6M-NAJ6>.

[196] See, eg, Katy Barnett, Kenneth Yin and Martin Allcock, *Remedies Cases and Materials in Australian Private Law* (Cambridge University Press, 2023) 174–6; Bryan, Vann and Barkehall Thomas (n 183) 205–7.

[197] See *Cth Privacy Act* (n 2) ss 13, 36; *ACT Privacy Act* (n 2) ss 11, 33–5; *NSW Privacy Act* (n 2) s 45; *NT Information Act* (n 2) ss 67, 104–5; *Qld Privacy Act* (n 2) ss 164–6; *Tas Information Protection Act* (n 2) s 18; *Vic Privacy Act* (n 1) ss 16, 57.

[198] This issue does not arise if the rights of access are sourced in contract; in that case, ordinary trust principles would apply: see Jeremiah Lau, James Penner and Benjamin Wong, 'The Basics of Private and Public Data Trusts' [2020] (1) *Singapore Journal of Legal Studies* 90, 106, 109.

There may very well be a role for trusts in legal arrangements made to benefit data subjects. However, at least in Australia, it is difficult to conceive of a scenario in which data governance could be promoted directly through a formal trust structure. Nevertheless, trusts could be used so that the benefit of contractual promises (which may include obligations with respect to storage and non-disclosure of data) can flow to the data subjects.

2 *Information Fiduciaries*

A related proposal to data trusts is the suggestion from US legal scholars that data custodians ought to be 'information fiduciaries' with respect to data subjects.[199] The *Digital Personal Data Protection Act 2023* (India) similarly uses the term 'Data Fiduciary' for persons who determine the 'purpose and means of processing of personal data' and thus the legislation associates obligations with that term.[200] However, the notion of 'fiduciary' deployed in the US literature and the Indian Act is quite different to the notion that is operating in Australia. Obligations such as a duty not to abuse data subjects' trust by, for example, violating privacy policies or a duty analogous to an obligation of confidence would not be considered fiduciary in nature in Australia.[201] Fiduciary obligations in Australia focus on loyalty through rules about conflicts of interest and profit-making rather than on positive obligations of care for others.[202] The proposal to deploying the concept of information fiduciaries to enhance data governance is thus unlikely to find traction in Australia and it has also been criticised on its own terms in the American context.[203]

[199] Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49(4) *University of California, Davis Law Review* 1183, 1186–7, 1209, 1221–5; Ariel Dobkin, 'Information Fiduciaries in Practice: Data Privacy and User Expectations' (2018) 33(1) *Berkeley Technology Law Journal* 1, 10–12.

[200] *Digital Personal Data Protection Act 2023* (India) ss 2(i), 4–10.

[201] See ibid; Balkin (n 199) 1209, 1223–4; Dobkin (n 199) 7, 17–18, 44–7.

[202] *Breen* (n 122) 83 (Brennan CJ), 94–5 (Dawson and Toohey JJ), 112–13 (Gaudron and McHugh JJ), 137–8 (Gummow J).

[203] See, eg, Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133(2) *Harvard Law Review* 497, 520–8, 534–7.

IV Governing Data through Contracts

A *Data Sharing Agreements in Australia*

As detailed above, data sharing regulation in Australia is based on general principles and vague obligations.[204] These general principles can be implemented by data sharing entities through data sharing agreements that can provide additional instructions and delineate concrete obligations with which the parties must comply.

Data sharing agreements serve several purposes. First and foremost, they ensure that data is shared consistently with the applicable laws and in compliance with the normative legislative framework.[205] Additionally, data sharing agreements ensure that entities that share data comply with information management standards and follow organisational data governance policies.[206] Therefore, contracts contain the concrete data sharing obligations and instructions under which data controlled by one entity ('data custodian') is transmitted or made available to another entity ('data recipient').[207] Data sharing agreements also reflect the organisational practices and culture concerning the handling of digital data.[208]

Because of the nature of some types of data (mainly personal information), where two (or more) organisations agree to share data, their agreement may affect the rights and duties of third parties (including data subjects). These third parties are not typically part of the contract and, accordingly, have no control

[204] See above nn 40–9 and accompanying text.

[205] The applicable laws are mainly data protection and data privacy laws: see above Part II(A). See generally Office of the National Data Commissioner, *Introducing the DATA Scheme* (n 51) 2–3.

[206] See, eg, 'Data Sharing Agreements', *Information Commissioner's Office* (Web Page) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements/>, archived at <https://perma.cc/LN46-MJX8>; Australian Research Data Commons, *Data Sharing Agreement Development Guidelines* (Guidelines, January 2023) 5 <https://zenodo.org/records/7553198>, archived at <https://perma.cc/7YCA-8N79>.

[207] See, eg, Office of the National Data Commissioner, *Data Sharing Agreement* (Agreement) 5–13 items 2–7 <https://www.datacommissioner.gov.au/sites/default/files/2022-07/ONDC_Legislation_Agnostic_DSA_Template.doc>, archived at <https://perma.cc/8A3B-9K8H> ('*ONDC Agreement*'). Such recipients are often referred to as 'users' or 'intermediaries': see, eg, ACT Government, *Data Sharing Agreement* (Agreement) 4 items 1.1–1.3 <https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0005/2194844/Internal-Data-Sharing-Agreement-Template.pdf>, archived at <https://perma.cc/V3M3-BMVA> ('*ACT Agreement*'); *ONDC Agreement* (n 207) 3–4 item 1.

[208] 'Data Sharing Agreements' (n 206).

over or effect on the contractual obligations.[209] In some circumstances, entry into the data sharing agreement is itself a breach of the data custodian's legal obligations under the *Privacy Act*.[210] Where statutory requirements are breached, statutory remedies may be available.[211] To be utilised, these statutory mechanisms currently require the support of the Office of the Australian Information Commissioner.[212]

The role of contracts in governing data sharing activities (and data governance more broadly) has led organisations and government bodies to develop data sharing agreement templates designed to guide and support entities engaged in data sharing.[213] These template agreements set out the main principles for data sharing, yet they often refrain from providing clear instructions, leaving much room for the parties to decide how to govern their data flows.[214] In Australia, the Office of the National Data Commissioner ('ONDC') created such a data sharing agreement template ('*ONDC Agreement*').[215] The *ONDC Agreement* template is a soft-law legal instrument designed to assist data sharing entities to better streamline their data sharing activities.[216] The template is a part of the developing data sharing framework and provides structure and recommendations regarding the legal

[209] See *Hobart International Airport Pty Ltd v Clarence City Council* (2022) 276 CLR 519, 538–9 [34] (Kiefel CJ, Keane and Gordon JJ), 552–3 [70]–[71] (Gageler and Gleeson JJ), 558 [86], 569–70 [119]–[121] (Edelman and Steward JJ) ('*Hobart International Airport*'). However, under 'exceptional circumstances', a person who has a strong interest in the operation of a contract to which they are not a party may have legal standing to seek a declaration about the meaning of the contract: at 539 [35] (Kiefel CJ, Keane and Gordon JJ), 552–4 [70]–[73] (Gageler and Gleeson JJ), 570–1 [121]–[122] (Edelman and Steward JJ).

[210] See *Australian Privacy Principles* (n 70) cls 6.

[211] *Cth Privacy Act* (n 2) ss 13G, 25–25A, 80U(1).

[212] Ibid ss 36–50, 52, 80U(2).

[213] See below Part VII. See also Productivity Commission, *Data Availability* (n 3) 269–70.

[214] See, eg, *ONDC Agreement* (n 207) 5–13 items 2–7.

[215] *ONDC Agreement* (n 207).

[216] Ibid. This template is indeed assisting data sharing processes across Australia; the *ACT Agreement* (n 207) closely emulates the approach and structure of the template: at 2. See also Gayle Milnes, 'National Data Commissioner Update: February 2023', *Office of the National Data Commissioner* (Web Page, 28 February 2023) <https://www.datacommissioner.gov.au/node/165>.

considerations that data sharing entities should include in their agreements.[217] It is currently undergoing revision.[218]

To better understand how data sharing agreements are drafted and operate in practice, we reviewed the language and content of 23 data sharing agreements and agreement templates used in Australia and internationally (by both public and private entities).[219] While our observations are based on a small sample and the number and types of data sharing agreements we examined are not representative of data sharing agreements everywhere, our observations provide insight into existing practices. Our analysis of these data sharing agreements also suggests that there are significant gaps in the current coverage of those agreements and the role they play in data sharing in Australia.

Our analysis focuses on three elements in data sharing agreements: a commitment to protect data subjects' rights, language and terminology, and specificity and comprehensiveness.

1 *Data Subjects' Rights*

Data sharing agreements are bilateral or multilateral contracts between organisations sharing data and organisations gaining access to data.[220] Therefore, these contracts represent the interests and bargaining power of the contracting parties albeit within the constraints of privacy and data sharing legislation.[221] Generally, for negotiated terms, data subjects' interests are represented only (a) through the general legal principles enshrined in the regulatory framework and (b) where they align with the contracting parties' interests, including their interest in maintaining their reputation. Data subjects are often greatly affected by breaches but are rarely party to, or consulted on,

[217] *ONDC Agreement* (n 207) 5–12. See also Office of the National Data Commissioner, *Introducing the DATA Scheme* (n 51) 1, 3–4; Milnes (n 216).

[218] The authors were invited to consult with the Office of the National Data Commissioner team on appropriate revisions to the template on 26 May 2022.

[219] Overall, we reviewed 23 publicly available data sharing agreements and templates in Australia and other jurisdictions (including New Zealand, the European Union, the United Kingdom and the United States). The agreements reviewed include data sharing in a variety of contexts (such as health data, education data and housing data) and cover both government and non-government data sharing activities: see below Part VII.

[220] 'Data Sharing Agreements' (n 206); Caimi et al (n 15) 179, 182. See, eg, *ACT Agreement* (n 207) 4.

[221] See above nn 206–7, 213–14 and accompanying text. See also Robert L Hale, 'Bargaining, Duress, and Economic Liberty' (1943) 43(5) *Columbia Law Review* 603, 605.

the agreement and its terms.[222] This means that data sharing agreements may include clauses with negative practical consequences for data subjects without their agreement beyond the initial 'consent' required in some circumstances under privacy legislation.[223]

Consistently with Australian law, none of the six Australian public sector data sharing agreements we examined included explicit references to data subjects' rights or guaranteed their protection (beyond the basic legal requirement of consent).[224] Data subjects are not considered parties (or interested third parties) in the structure of these data sharing agreements and are therefore not accorded concrete rights (such as rights to access, correction or erasure of their data) or avenues to respond to contract breaches that directly affect them.[225] This approach will only increase data protection illiteracy and weaken individuals' confidence in government agencies engaged in the collection of data.[226] While involving data subjects directly in negotiations may

[222] See, eg, Office of the Australian Information Commissioner, *Notifiable Data Breaches Report* (Report, 5 September 2023) 10–12 <https://www.oaic.gov.au/__data/assets/pdf_file/0020/83702/OAIC-Notifiable-data-breaches-report-January-to-June-2023-final.pdf>, archived at <https://perma.cc/JR3V-KHXM>; Office of the Australian Information Commissioner, *Community Attitudes* (n 27) 10. However, the entity controlling the data and the entity receiving the data (and, if applicable, any intermediaries) are generally the only parties to the data sharing agreement: see, eg, *ONDC Agreement* (n 207) 3–4 item 1; *ACT Agreement* (n 207) 4 items 1.1–1.3.

[223] See, eg, *Australian Privacy Principles* (n 70) cl 6.1(a); *ACT Privacy Act* (n 2) sch 1 principle 6.1(a); *NSW Privacy Act* (n 2) ss 10, 17(a); *NT Information Act* (n 2) sch 2 principles 1–2; *Qld Privacy Act* (n 2) sch 3 ss 2, 10(1)(a); *Tas Information Protection Act* (n 2) sch 1 cls 1–2; *Vic Privacy Act* (n 1) sch 1 cls 1–2.

[224] We looked at the following six templates and agreements: see *ONDC Agreement* (n 207) 6–7 item 4.2; *Intergovernmental Agreement* (n 1) 3 cl 2(d)(iv); *ACT Agreement* (n 207) 11 item 7; Department of Customer Service (NSW), *Data Sharing Agreement Generator User Guide (Prototype V2)* (Guide, 5 November 2019) 22 cl 3 <https://data.nsw.gov.au/sites/default/files/2019-11/DSA%20Generator%20User%20Guide%20-%20approved.pdf>, archived at <https://perma.cc/2K5L-ZBB4> ('*NSW Agreement*'); Department of the Premier and Cabinet (SA), *Data Sharing Agreement between South Australian Government/Non-Government* (Agreement) 6 cl 6 <https://www.dpc.sa.gov.au/__data/assets/pdf_file/0017/47330/Data-Sharing-Agreement-government-nongovernment-template-2022.pdf>, archived at <https://perma.cc/NSK7-UHDB> ('*SA Agreement*'); Victoria State Government, *Victorian Public Sector (VPS) Data Sharing Heads of Agreement* (Agreement) cls 8–10 <https://content.vic.gov.au/sites/default/files/2022-08/Victoria%20Public%20Sector%20Data%20Sharing%20Heads%20of%20Agreement%20-%20as%20at%2019%20August%202022.pdf>, archived at <https://perma.cc/F5JS-8WBQ> ('*Vic Agreement*').

[225] See *ONDC Agreement* (n 207); *Intergovernmental Agreement* (n 1); *ACT Agreement* (n 207); *NSW Agreement* (n 224); *SA Agreement* (n 224); *Vic Agreement* (n 224).

[226] See Office of the Australian Information Commissioner, *Community Attitudes* (n 27) 6, 9, 16.

not be practicable, the template should be drafted and used, particularly by government agencies, in ways that protect the interests of data subjects and enhance data governance. Below, we discuss how this can be done in ways that provide practical protection for data subjects.

Of the two non-government Australian data sharing agreement templates we inspected — one created by Monash Partners Academic Health Science Centre ('Monash Partners') and the other created by the Australian Broadcasting Company ('ABC') — the ABC's template similarly refrains from explicitly mentioning data subjects' rights.[227] Instead, it includes general provisions requiring the data recipients to comply with 'all applicable laws', including 'any applicable Privacy Laws'.[228] In contrast, Monash Partners' template includes an explicit reference to patients' rights.[229]

As expected, European templates — including the *GDPR*-compliant *Data Processing Agreement* template that governs data sharing between data controllers and data processors — provide an alternative.[230] The *Data Processing Agreement* template devotes several of its sections to the obligations of the contracting parties towards data subjects.[231] These obligations include ensuring that requests to exercise data subjects' rights are properly responded to and informing data subjects of any breaches involving their personal data.[232] While the clear inclusion of data subjects' rights corresponds with the inclusion of such rights in the regulatory framework — the *GDPR* itself — it is of course possible to envision the inclusion of data subjects' rights even in the absence of statutory rights in the Australian context (eg in the spirit of the Monash Partners' template).[233] The data sharing template issued by the British

[227] See Australian Broadcasting Corporation, *Data Sharing Agreement: Australia Talks National Survey 2019* (Agreement, 2019) 4–7 cls 1–17 <https://about.abc.net.au/wp-content/uploads/2020/12/ABC-Data-Sharing-Agreement-DRAFT.pdf>, archived at <https://perma.cc/BE6D-UWQV> ('*ABC Agreement*').

[228] Ibid 4 cl 3.5(a).

[229] Alison Johnson and Helena Teede, Monash Partners Academic Health Science Centre, *Data Sharing Agreement and Principles* (Agreement, July 2021) 30–1 s 5.4 <https://bridges.monash.edu/articles/online_resource/Monash_Partners_Data_Sharing_Agreement_and_Principles/14825616>, archived at <https://perma.cc/HYC8-ESPU> ('*Monash Partners Agreement*').

[230] *Data Processing Agreement* (Agreement) <https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf>, archived at <https://perma.cc/LEE2-44NQ>.

[231] Ibid ss 6–7.

[232] Ibid.

[233] Ibid; *GDPR* (n 5) arts 12–23, 34; *Monash Partners Agreement* (n 229) 30–1 s 5.4. See above Part II(B)(1).

Information Commissioner's Office similarly contains references to data subjects' rights and instructs entities that share data to specify procedures that allow data subjects to exercise their individual rights easily (though the template and its supporting documents provide limited guidance on how this goal should be achieved).[234]

2 *Language and Terminology*

While we find that many data sharing agreements — in Australia and internationally — are adopting clear and accurate terms, we identify a few recurring problems. One core issue relates to ownership or property terminology; this issue mirrors the terminological ambiguity in the legislation.[235] This terminology signals that a single party (ie the one that 'owns' or has property in the data) may be responsible for data protection or authorised to share the data. The New South Wales ('NSW') template, for example, unhelpfully includes the following as a core question to the data provider: 'Does your agency own the data?'[236] The template then specifies that if the answer to this question is 'No', then the agreement is to be disqualified, presumably because the only party authorised to share the data is the party that 'owns' it.[237] This is despite the fact that, as explained above, no government agency technically owns data under Australian law.[238] Similarly, the Monash Partners' template defines the Chief Executive of each organisation as the 'Data Owner'.[239] While it seems that this terminology is used to indicate who has the authority to disclose the relevant data, it is nonetheless confusing and legally inaccurate. Another example is the Sydney Harbour ferry system contract for the provision of ferry services which stipulates that 'all information and data collected by the Electronic Ticketing System … is the property of the Director-General [of the NSW Department of Transport] or the Director-General's Associate', thus it inaccurately invokes property law.[240] Similarly, a recent

[234] See *UK Agreement* (n 1) 28–9, 48–52, 84, 89.

[235] See above nn 52–4 and accompanying text.

[236] *NSW Agreement* (n 224) 14.

[237] Ibid.

[238] See above nn 121–30 and accompanying text.

[239] *Monash Partners Agreement* (n 229) 30 s 5.3.

[240] MinterEllison Lawyers, *Ferry System Contract* (Contract) 53 cl 10.9(f) <https://www.transport.nsw.gov.au/sites/default/files/media/documents/2017/ferry-system-contract_0.pdf>, archived at <https://perma.cc/3GUR-GWLV>. This contract has been

comprehensive guide on contract design for data sharing proposed the following language for an end-of-contract clause: 'All data transferred to [the data recipient] by [the data custodian] shall remain the property of [the data custodian]'.[241]

Similarly, the Victorian template seems to misuse the term 'rights' to reflect the permissibility of data sharing on the part of the entity that shares data.[242] The template requires that the data provider 'has all necessary rights and consents required, to disclose the Shared Data'.[243] While the consent of data subjects is indeed a necessary condition for most lawful data transfers,[244] it is not clear what 'rights' the data provider has in relation to such data.[245] Additionally, the Victorian template applies to actions to 'collect, hold, manage, use, disclose or transfer' data.[246] While attempting to cover a range of data-related actions, the specificity of those terms creates gaps around non-enumerated actions (such as 'access' and 'process') and raises the abovementioned concerns with regard to (admittedly statutory) terms suggesting physicality such as 'holds'.[247] The mix of confusing statutory and contractual terminology can affect the applicability of statutory protections. For example, where parties contractually agree that only one of them will have 'possession or control', this may impact which entity 'holds' the information for

positively cited as an 'example of a contract … that explicitly builds in an ownership right for government over the data collected by the provider': Productivity Commission, *Data Availability and Use* (Draft Report, October 2016) 187 <https://www.pc.gov.au/inquiries/completed/data-access/thedraft/data-access-draft.pdf>, archived at <https://perma.cc/Q9RR-8JPN>.

241 Andrew J Zahuranec, Hannah Chafetz and Stefaan Verhulst, *Moving from Idea to Practice: Three Resources for Harnessing the Power of Data Sharing Agreements* (Report, 2023) 22 <https://static1.squarespace.com/static/654501be298ff414eb84fa65/t/654517b98b7aad6b4aa8da57/1699026908451/A+Guide+to+Data+Sharing+Agreements.pdf>, archived at <https://perma.cc/HQ63-3RZ8>.

242 *Vic Agreement* (n 224) cl 11(a).

243 Ibid.

244 See, eg, *Australian Privacy Principles* (n 70) cl 6.1(a); *ACT Privacy Act* (n 2) sch 1 principle 6.1(a); *NSW Privacy Act* (n 2) ss 17–18; *NT Information Act* (n 2) sch 2 principle 2.1(c); *Qld Privacy Act* (n 2) sch 3 s 11(1)(b); *Tas Information Protection Act* (n 2) sch 1 cl 2(1)(b); *Vic Privacy Act* (n 1) sch 1 cl 2.1(b).

245 Note that, in Australia, data per se is not a thing to which property rights attach: see above Part III(A).

246 *Vic Agreement* (n 224) cls 8(c), 10(a), 12(b).

247 See above nn 52–4 and accompanying text.

the purposes of obligations under the *Privacy Act*.[248] The agreement thus changes the identity of the duty-holder.

The British Information Commissioner's Office template offers alternative terminology that can prevent the misuse of both the 'rights' and 'ownership' terminology referenced in other data sharing agreement templates. It instead adopts the term 'legal power' to refer to the authority to share the specified data.[249] The term 'legal power' does not relate to data ownership or property rights in the data but rather to the requirements of the overarching data privacy and data protection legislation.[250] It thus avoids the terminological confusion around ownership.

3 *Specificity and Comprehensiveness*

Most of the Australian data sharing agreements that we reviewed lacked both specificity and comprehensiveness, resorting to general principles and failing to include important obligations.[251] While vague or incomplete contracts may have some cost benefits in contract design, incompleteness in data sharing agreements poses significant costs in terms of contract enforcement and the protection of data subjects' rights.[252] An important data sharing element that was absent or vague in many Australian data sharing agreements relates to end-of-agreement obligations.[253] For example, while the Monash Partners' template requires parties to the data sharing agreement to specify 'the agreed time-period for retaining the data and the data disposal plan', the template does not include recommended actions and allows the parties to note that a data retention and disposal plan is '[u]nknown'.[254] An exception to this end-of-agreement problem is the Victorian template which clearly instructs that shared

[248] *Cth Privacy Act* (n 2) s 6(1) (definition of 'holds'); *Australian Privacy Principles* (n 70) cls 6–7, 11–13.

[249] *UK Agreement* (n 1) 84.

[250] See ibid 28–9, 39–41.

[251] See below Part VII.

[252] Wendy Netter Epstein, 'Facilitating Incomplete Contracts' (2014) 65(2) *Case Western Reserve Law Review* 297, 306–12.

[253] See, eg, *ONDC Agreement* (n 207) 5–6 item 3; *Intergovernmental Agreement* (n 1) 5 cl 10; *ACT Agreement* (n 207) 12 item 8; *NSW Agreement* (n 224) 11, 29; *SA Agreement* (n 224); *ABC Agreement* (n 227) 6 cl 14; *Monash Partners Agreement* (n 229) 63. Cf *Data Processing Agreement* (n 230) s 9.

[254] *Monash Partners Agreement* (n 229) 53, 63, 77.

data must be disposed of as soon as the purpose for which it was shared is fulfilled (unless otherwise required by law).[255]

Another identified gap relates to effective enforcement mechanisms. Clauses in data sharing agreements that can potentially benefit data subjects lack effective enforcement mechanisms for third parties such as data subjects.[256] Instead, data custodians (or contracting parties) assume the role of de facto regulators and design the contractual scheme based on their interests and concerns; additionally, data custodians assess their own application and compliance under the contractual scheme.[257] This means that some issues remain unaccounted for, especially when those issues do not pose a concern for any of the contracting parties. This is particularly concerning considering that the data custodian has conflicting interests and responsibilities affecting their incentives to monitor and enforce compliance.[258] The ONDC, Australian Capital Territory, NSW, SA and Victorian templates all fail to designate a conflict resolution mechanism or fail to include a requirement to conduct specific follow-up actions in response to data breaches (beyond a data breach notification).[259]

In contrast, several (though not all) of the international data sharing agreements we reviewed contained specific instructions for data retention and data destruction as well as specific mechanisms for conflict resolution and redress. For example, X (formerly Twitter) requires a controller to delete data shared with it within ten days of receiving a written request from X or when the purpose of the data sharing expires.[260] Similarly, the US State of Washington's Office of Superintendent of Public Instruction specifies in their data sharing agreement template that a '[c]ontractor agrees to destroy all data within forty-

255 *Vic Agreement* (n 224) cl 13.

256 Although declaratory relief is available in exceptional circumstances: see *Hobart International Airport* (n 209) 538–41 [34]–[41] (Kiefel CJ, Keane and Gordon JJ), 552–5 [70]–[77] (Gageler and Gleeson JJ), 569–71 [120]–[123] (Edelman and Steward JJ).

257 See Zahuranec, Chafetz and Verhulst (n 241) 4.

258 See Productivity Commission, *Data Availability* (n 3) 141–2.

259 See *ONDC Agreement* (n 207) 12 item 5.1; *ACT Agreement* (n 207); *NSW Agreement* (n 224) 26 cl 12(f); *SA Agreement* (n 224); *Vic Agreement* (n 224).

260 'X Controller-to-Controller (Outbound) Data Protection Addendum', *X GDPR* (Web Page, 2024) s 3 <https://gdpr.twitter.com/en/controller-to-controller-transfers.html>, archived at <https://perma.cc/D5ZY-VJMT> ('X Agreement').

five (45) days after it is no longer needed'.[261] In the US, the Council of Large Public Housing Authorities requires housing authorities and education organisations to permanently destroy all student data shared with it when the data is no longer necessary for the purposes of the data sharing agreement.[262] The template also requires the data recipient to document and provide certification that the data has been destroyed.[263] Meta's data processing terms similarly specify that 'Meta shall delete the Personal Information within the period set forth in the Applicable Product Terms, unless applicable law requires further storage'.[264] However, a data sharing agreement template involving Facebook, the *Research Data Agreement*, does not specify any concrete or detailed end-of-agreement obligations.[265]

Regarding dispute resolution and enforcement mechanisms, the *GDPR*-compliant *Data Processing Agreement* template instructs the contracting parties to agree on a dispute resolution body and jurisdiction and to specify obligations in response to personal data breaches (including to investigate, mitigate and remediate each such breach).[266] It further instructs the parties to conduct data protection impact assessments.[267] The Facebook *Research Data Agreement* requires parties to the agreement to consider a variety of dispute resolution mechanisms developed for data protection disputes, including arbitration and mediation.[268]

[261] *Agreement between Requestor and the Office of Superintendent of Public Instruction to Authorize the Release and Use of Identifiable Student-Level Data* (Agreement) 2 <https://eds.ospi.k12.wa.us/iGrants/docs/19-20/FormPackages/State/WaKIDS744/Data%20Share%20Agreement.pdf>, archived at <https://perma.cc/3AS7-4PFR> (*'US Office of Superintendent Agreement'*).

[262] Council of Large Public Housing Authorities, 'Aligning Education and Housing: Data Sharing Agreement Template', *Housing Is* (Web Page, 1 May 2016) ss 1(i), 2(b) <https://housingis.org/content/aligning-education-and-housing-data-sharing-agreement-template>, archived at <https://perma.cc/Z5QF-4ZS8> ('*Council of Housing Authorities Agreement*').

[263] Ibid.

[264] 'Data Processing Terms', *Facebook* (Web Page, 25 April 2023) cl 6 <https://www.facebook.com/legal/terms/dataprocessing>, archived at <https://perma.cc/3SZL-HDMQ>.

[265] *Research Data Agreement* (Agreement) s 5(b), sch 1 s 4 <https://socialscience.one/sites/projects.iq.harvard.edu/files/socialscienceone/files/fort_non-monetary_rda_with_public_institution_and_developer_terms.pdf>, archived at <https://perma.cc/PBL7-ZS5R> ('*Facebook Research Agreement*').

[266] *Data Processing Agreement* (n 230) ss 7, 13.

[267] Ibid s 8.

[268] *Facebook Research Agreement* (n 265) sch 1 exhibit 1 cl 6.2.

B *Contracting for Better Data Governance*

To address the problems identified above without changing core legal concepts and frameworks, we propose changes to Australia's data sharing agreement template — and data sharing agreements generally — based on a 'data governance approach' inspired by innovations in contract law and informed by our review of different data sharing agreements (including the *GDPR*-compliant *Data Processing Agreement* template and the approach taken by the EU's *DGA*).[269] Our recommendations focus on strengthening data governance through proposed changes to data sharing agreements that reflect the potential impact of data sharing on individuals' digital identity, privacy and autonomy.

To address the structural concerns raised above, including those about contractual harms inflicted upon third parties (such as data subjects), we propose the inclusion of data subjects' interests within the ecosystem of data sharing governance through contracts. Scholars have already posited that third parties should be considered to be a part of the contract ecosystem, and that, accordingly, contract law should limit not just the harms imposed by contracting parties on each other but also the harms jointly imposed by contracting parties on third parties.[270] In the context of supply chain contracts that may harm third parties' human rights, Kishanthi Parella suggests that protecting third parties from harm can be achieved through contract design by requiring parties to the contract to take into account the interests of third parties and to incorporate those interests into the contract.[271] Indeed, the United Nations *Guiding Principles on Business and Human Rights* ('*UNGP*') require businesses to actively communicate their commitment to meet their responsibility to protect human rights 'to entities with which the enterprise has contractual relationships'.[272] Another more general route is to include human rights due diligence obligations in the contract, in line with the *UNGP* requirement to initiate human rights due diligence as early as possible 'given

[269] See *Data Processing Agreement* (n 230); *DGA* (n 5) recitals 5–7, art 1.

[270] See, eg, Aditi Bagchi, 'Other People's Contracts' (2015) 32(2) *Yale Journal on Regulation* 211, 241–6, 255; Kishanthi Parella, 'Protecting Third Parties in Contracts' (2021) 58(2) *American Business Law Journal* 327, 328–9, 351–2.

[271] Parella (n 270) 351–5, 383.

[272] Human Rights Council, *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/31 (21 March 2011) annex ('*Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*') 15.

that human rights risks can be increased or mitigated … at the stage of structuring contracts or other agreements'.[273] While this proposition may increase contract design costs, it has enforcement (or verification) benefits in a complex data governance environment (especially if these terms are incorporated into national templates).[274]

Following the developments concerning contracts that affect third parties, we propose that data sharing agreements should acknowledge the potential effects of the contracted data sharing activities on data subjects and incorporate concrete measures to strengthen data governance and enhance data protection. These measures may include de-identification, anonymisation and redaction as well as internal processes to allow data subjects to raise concerns and request information.[275] (These internal processes are similar to the requirement under the *Data Processing Agreement* template to implement 'appropriate technical and organisational measures' to respond to data subjects' requests for information and to exercise their rights under the relevant legislation.)[276] As noted above, the Australian regulatory approach to data sharing bestows fewer rights (or powers) upon data subjects than the *GDPR*.[277] While amending this approach requires comprehensive law reform (some of which is already underway),[278] data sharing agreements can mitigate this problem by generating clear and comprehensive data governance tasks and responsibilities. This approach still leaves data subjects outside of contractual relations (and maintains the position of data sharing entities as de facto regulators), but, at the same time, it acknowledges data subjects' interests and requires the contracting parties to create organisational pathways to actively engage with data subjects and to consider their interests.

[273] Ibid 16.

[274] See Albert Choi and George Triantis, 'Strategic Vagueness in Contract Design: The Case of Corporate Acquisitions' (2010) 119(5) *Yale Law Journal* 848, 852, 883–4. Cf Robert E Scott and George G Triantis, 'Anticipating Litigation in Contract Design' (2006) 115(4) *Yale Law Journal* 814, 822–34.

[275] See Information Commissioner's Office (UK), *Anonymisation: Managing Data Protection Risk* (Code of Practice) 12–13, 22, 58 <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>, archived at <https://perma.cc/2TVV-959J>; Information and Privacy Commission (NSW), *De-Identification of Personal Information* (Fact Sheet, May 2020) 1–2 <https://www.ipc.nsw.gov.au/sites/default/files/2021-03/Fact_Sheet_De-identification_of_personal_information_May_2020.pdf>, archived at <https://perma.cc/4TZG-L439>.

[276] *Data Processing Agreement* (n 230) s 6.1.

[277] See above Part II(B). Cf *GDPR* (n 5) arts 12–23.

[278] See above n 67 and accompanying text.

Specifically, we propose to enhance the data governance framework of the *DAT Act* through a revised data sharing agreement template.[279] The revised template should include concrete obligations and responsibilities designed to minimise harm to data subjects, including through advanced de-identification techniques conducted by trusted intermediaries, added transparency and dialogue with civil society and human rights organisations. An acceptable de-identification technique might include 'red teaming' to test the re-identifiability of information.[280] This approach could be further strengthened by establishing a clear risk assessment method to evaluate the risks (including reidentification risks) and benefits expected from the data sharing activities.[281] Our proposal is also consistent with the approach taken by the *DGA*.[282]

These safeguards will serve the Australian public on three levels — by enhancing the ability to use public data for the public good,[283] by promoting data-driven solutions for 'wicked' global challenges[284] and by increasing the public's confidence in government data sharing, including under the *DAT Act* scheme.[285] The expected benefit of these safeguards is that 'safe' data flows will be encouraged while ensuring additional governance hurdles to better protect individuals' privacy and autonomy in situations where sharing does involve greater risk to personal information. [286]

279 See generally *Cth DAT Act* (n 1).

280 See Joseph V DeMarco, 'An Approach to Minimizing Legal and Reputational Risk in Red Team Hacking Exercises' (2018) 34(4) *Computer Law and Security Review* 908, 908–9; Rebecca Balebako, 'Privacy Red Teams: The Why and How of an Emerging Privacy Practice', *Privacy Engineer* (Blog Post, 21 May 2023) <https://medium.com/privacy-engineer/privacy-red-teams-the-why-and-how-of-an-emerging-privacy-practice-a37827ef95cf>, archived at <https://perma.cc/XES6-GGEY>. For additional de-identification techniques, see Inge Graef and Jens Prüfer, 'Governance of Data Sharing: A Law & Economics Proposal' (2021) 50(9) *Research Policy* 104330:1–14, 9–10; *DGA* (n 5) recital 7.

281 See Luc Rocher, Julien M Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 *Nature Communications* 3069:1–9, 2–6.

282 *DGA* (n 5) recitals 5–7, art 1.

283 See, eg, *Intergovernmental Agreement* (n 1) 1–2.

284 Susan Ariel Aaronson, 'Wicked Problems Might Inspire Greater Data Sharing' (Working Paper No 9/2022, Elliott School of International Affairs, The George Washington University, September 2022) 1.

285 For an approach that focuses on the trustworthiness of the data sharing scheme, see *DGA* (n 5) recitals 3, 5, 32, 38.

286 This is in line with the objectives of the *Cth DAT Act* (n 1) s 3.

Finally, to address the substantive legal gaps and inadequate legal terminology in data sharing contracts, we further propose that data sharing agreement templates include clear references to the applicable legislation and the compliance obligations of the contracting parties.[287] Best practice rules (or minimum standards) should also be listed to enhance compliance with the regulatory framework, to clarify and elaborate concrete obligations (rather than vague principles) and to set recommended actions designed to minimise risk. To strengthen organisational data governance culture, we propose that data sharing agreement templates adopt suitable legal terms that highlight the digital nature of data.[288] For example, property-like terminology such as 'own' or 'possess' should be avoided and other potentially confusing terms such as 'hold' should only be used where necessary to mirror statutory terminology.[289]

These improvements can be embraced *without* changing Australia's privacy legislation. While they draw some inspiration from the approach adopted by the EU, they do not depend on reforms to Australian data privacy legislation.[290]

V Improving Data Governance in the Context of Data Sharing

In an increasingly digitised world, data sharing activities are both necessary and inevitable.[291] However, data sharing practices entail a variety of risks, including those related to individuals' identity, privacy and autonomy.[292] Different countries and organisations have adopted various approaches to ensure that their data sharing activities appropriately balance the benefits and risks associated with data sharing.[293] In Australia, the main legal instrument that

287 See above Part II(A).

288 For a discussion about the nature of digital files, see Michels and Millard, 'The New Things' (n 131) 329–32.

289 See above nn 52–6 and accompanying text. See also Bennett Moses (n 53) 631.

290 See above Part II(B).

291 See Australian Computer Society, 'Introduction: Why We Should Care' in Australian Computer Society (ed), *Data and the Digital Self: What the 21st Century Needs* (Report, February 2023) 2, 2–3 <https://www.acs.org.au/insightsandpublications/reports-publications/data-and-the-digital-self.html>, archived at <https://perma.cc/G5UJ-T5X2>.

292 See Danielle Keats Citron and Daniel J Solove, 'Privacy Harms' (2022) 102(3) *Boston University Law Review* 793, 830–61; Rachel L Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth et al (eds), *European Data Protection: Coming of Age* (Springer, 2013) 3, 10–24, 28.

293 See, eg, Custers et al (n 85) 240; *Facebook Research Agreement* (n 265).

governs sharing activities is contract; in this context, contracts are loosely regulated by two separate legal frameworks — data privacy and data sharing — that vary depending on the jurisdiction, the data sharing entities and the types of shared data.[294] The complexity and inconsistency of this layered and localised legislation, combined with the bilateral and ad hoc nature of data sharing contracts, generate insufficient guidance to direct data sharing entities and leaves data subjects largely outside of the data sharing ecosystem.[295]

While we believe that Australia's data sharing regime can be significantly improved through law reform (especially through revising and harmonising the data sharing legislation and the upcoming revision of the *Privacy Act*),[296] contract-based solutions can be applied immediately and voluntarily.

It is beyond the scope of this article to discuss, in depth, contract law theories concerning social values and social responsibility. However, contract-based solutions to social problems are neither new nor revolutionary and have been adopted in various contexts including human trafficking, environmental sustainability, and diversity and inclusion.[297] Courts have interpreted contract terms to mitigate harm or injury to third parties and contract theory has developed to acknowledge concepts of justice and social value.[298] Therefore, considering the possible effects of contracts on non-parties is an essential development in the interpretation and application of contracts in a complex and highly digitised world. We believe that data sharing contracts should evolve to reflect their inherent effects on individuals' privacy and autonomy and that

[294] Davis and Marotta-Wurgler (n 164) 663. See above nn 37–8 and accompanying text. To strengthen this legislation and to improve the balance between the benefits and harms associated with data sharing activities, Serena Syme Hildenbrand proposes various ways in which human rights laws (such as those in Queensland, Victoria and the Australian Capital Territory) can provide additional protections to data subjects in relevant jurisdictions: see, eg, Serena Syme Hildenbrand, 'Public Sector Data Sharing: Applying State-Based Human Rights Laws to Minimise Privacy Harms' (2024) 47(2) *Melbourne University Law Review* (advance), 32–41; Serena Syme Hildenbrand, 'Robodebt and Novel Data Technologies in the Public Sector: How Human Rights Laws Plug Data Protection Gaps' (2024) 43(2) *University of Queensland Law Journal* (advance), 14–38.

[295] See above Part IV(A).

[296] See above n 67 and accompanying text.

[297] See generally Jonathan C Lipson, 'Promising Justice: Contract (as) Social Responsibility' [2019] (5) *Wisconsin Law Review* 1109, 1109–13.

[298] Bagchi (n 270) 212, 241–6; JJ Spigelman, 'From Text to Context: Contemporary Contractual Interpretation' (2007) 81(5) *Australian Law Journal* 322, 335. See generally Hanoch Dagan and Avihay Dorfman, 'Just Relationships' (2016) 116(6) *Columbia Law Review* 1395, 1412, 1425–6.

national data sharing agreement templates and other guidance should encourage and model this change.[299] In essence, we call for a 'data governance approach' to data sharing contracts that reflects an awareness of the unique nature of these contracts and their potential effects on data subjects. This approach transcends the ad hoc nature of existing data sharing agreements and would integrate data subjects' interests and concerns into each data sharing transaction. It further dictates how data is to be processed and shared, what laws should be complied with and how compliance (in its broader non-technical sense) is to be achieved through setting specific recommended actions and obligations regarding data subjects.[300]

This approach is also consistent with the developing conceptualisation of data 'trusts' as a metaphor designed to increase *trust*worthiness through better contracts (rather than as an equitable doctrine).[301] Understood in this way, the new metaphorical or contractual data 'trusts' can improve data sharing practices through better governance arrangements that include trusted intermediaries. Indeed, some proposals use the language of 'data trust' not in the equitable sense discussed above but rather in a metaphorical sense.[302] The United Kingdom has expressed particular interest in these metaphorical 'data trusts', clarifying that '[t]rust law is not an appropriate legal structure for data trusts'[303] and that '[t]hese [data] trusts are not a legal entity or institution, but rather a set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data in a fair, safe and equitable way'.[304] The idea is to introduce a new organisation that would support, broker, standardise and oversee those agreements rather than to create a mechanism that would treat data as property.[305] The 'data trust' concept has also come up in the context of the now-abandoned Sidewalk Labs proposal for a smart city in Toronto's Quayside.[306] In that proposal, a civic data trust was described as '[a]n

[299] See, eg, Zahuranec, Chafetz and Verhulst (n 241) 8, 19–20.

[300] See above nn 7–11 and accompanying text.

[301] See Lau, Penner and Wong (n 198) 93; Delacroix and Lawrence (n 181) 242; *Data Trusts* (n 23) 8.

[302] Lau, Penner and Wong (n 198) 91–3.

[303] *Data Trusts* (n 23) 8.

[304] Hall and Pesenti (n 182) 46.

[305] Ibid 46–8.

[306] Sidewalk Labs (n 1) 12–13; Jordan Pearson, 'After Years of Big Promises, Sidewalk Labs Abandons Its Smart City in Toronto', *Vice* (Web Page, 7 May 2020) <https://www.vice.com/en/article/sidewalk-labs-abandons-its-smart-city-in-toronto/>, archived at <https://perma.cc/JJE2-WHM6>.

independent entity to control, manage, and make publicly accessible all data that could reasonably be considered a public asset, and a set of rules that would apply to all entities operating in Quayside, including Sidewalk Lab'[307] and 'a model for stewardship and management of data and digital infrastructure that approves and controls the collection and use of data for the benefit of society and individuals'.[308] Under the proposal, data would have been managed (or governed) by an independent third party with a charter focusing on public benefit, but there is no suggestion that the independent third party would have taken on the obligations of a trustee.[309] Indeed, the proposal explicitly claimed that it would have helped avoid the 'private ownership of data'.[310]

There are concerns about assigning the label 'data trusts' to legal arrangements other than trusts. There are differences between the rights that data subjects would have as beneficiaries of a trust, including being owed fiduciary obligations and being able to enforce their rights against third parties in some circumstances, and rights pursuant to contract.[311] Using the language of 'trust' could thus be misleading. While the word 'trust' is used in a different sense, as in the World Economic Forum's statement that 'it is necessary to develop a governance structure for data marketplaces, one that ensures trust',[312] the ambiguity inherent in the term 'data trust' is problematic.

Ultimately, data trusts in this sense are about an outcome — trustworthiness — that might be achieved through contractual governance arrangements that data subjects can *trust* to protect their rights and interests. In other words, the language of trust is being used to reframe the data sharing landscape and relationships, highlighting that bilateral or multilateral contracts not only affect data subjects deeply but also require their trust and participation in the new data economy. We agree with discussions relating to data sharing contracts reorientating from an exclusive focus on the interests of parties towards incorporating broader data governance responsibilities that respect the

307 Sidewalk Labs (n 1) 10.

308 Ibid 12.

309 Ibid 12–13.

310 Ibid 13.

311 See Marinotti (n 79) 153–7; *Hospital Products Ltd v United States Surgical Corporation* (1984) 156 CLR 41, 73 (Gibbs CJ), 97 (Mason J), 118–19 (Wilson J), 123–4 (Deane J), 147 (Dawson J).

312 Centre for the Fourth Industrial Revolution Japan, World Economic Forum, *Developing a Responsible and Well-Designed Governance Structure for Data Marketplaces* (Briefing Paper, August 2021) <http://www3.weforum.org/docs/WEF_DCPI_Governance_Structure_Towards_Data_Exchanges_2021.pdf>, archived at <https://perma.cc/8NKW-ZJXW>.

interests of data subjects and build *trust*.[313] Indeed, our suggestions for changes in data sharing agreement templates are based on this thinking. However, we believe that the language of 'data trusts' is ultimately confusing and unhelpful as a term to describe this reorientation; this shift is better captured through the terminology of data governance.

VI Conclusion

In this article, we considered three paths that would help address the tension between, on the one hand, permitting, or indeed promoting, beneficial forms of data sharing and, on the other hand, protecting the rights and interests of data subjects through better data governance arrangements.

The first path — reforming data privacy and data sharing regulation — is ambitious.[314] The reform of privacy legislation, including changes based on the *GDPR*, is being developed and we encourage the government to centre data subjects' rights in any proposed law reform.[315]

The second path — leveraging private law doctrines other than contract, including through considering the possibility of data propertisation — would require a significant upheaval of Australian law and would not offer significant benefits. Unlike reforming the *Privacy Act*, it has no current local traction, though we should follow developments elsewhere if these kinds of arrangements gain in popularity and we should keep an open mind to future law reform.[316] However, the metaphorical conceptualisation of 'data trusts' is linked to our third path (better contracts) because it reimagines contract-based data sharing arrangements from the perspective of trustworthy data governance.[317]

[313] See above nn 301–10 and accompanying text.

[314] See, eg, Lyria Bennett Moses and Kimberlee Weatherall, 'Data Problems and Legal Solutions: Some Thoughts beyond Privacy' in Australian Computer Society (ed), *Data and the Digital Self: What the 21st Century Needs* (Report, February 2023) 18, 26–9 <https://www.acs.org.au/insightsandpublications/reports-publications/data-and-the-digital-self.html>, archived at <https://perma.cc/G5UJ-T5X2>. Our characterisation of the first path as ambitious is particularly apt if reform is to involve changes to Australia's human rights framework to bring the Australian regulatory landscape more in line with that of the EU: see above Part II(B)(1). See also George Williams, *A Charter of Rights for Australia* (University of New South Wales Press, 3rd ed, 2007) 66–8.

[315] See above Part II(B).

[316] See above n 172 and accompanying text.

[317] See above nn 301–10 and accompanying text.

This third path — enhancing data governance through better contracts — does not rely on law reform and can be adopted immediately by both government bodies and industry parties engaged in data sharing activities. It can be modelled by the government through changes to the *ONDC Agreement* template.[318] Essentially, it involves drafting data sharing agreements with the objective of creating a trustworthy and concrete data governance environment that acknowledges and protects data subjects' identities, privacy and autonomy. We have suggested several ways in which existing data sharing agreements can be improved: (a) empowering data subjects and enhancing digital literacy by including data subjects in the structure of data governance mechanisms, (b) clarifying data sharing entities' responsibilities and obligations through more accurate terminology that is appropriate for digital data and (c) mitigating gaps in data protection and simplifying data governance through comprehensive and precise data sharing templates (beyond general principles). These proposals would allow organisations to realise common marketing statements that claim, in effect, that they 'value' your privacy.[319]

In conclusion, we encourage Australian governments to give careful consideration to law reform ideas. The most promising ideas are the proposed reforms to privacy legislation that are already under consideration.[320] Secondly, organisations entering into data sharing arrangements should not wait for such reform but should act now to embed data governance concerns into relevant contracts, paying careful attention both to the existing gaps that we identified in current practices and to our proposed solutions.[321] The federal government can lead the way through data sharing templates, but all organisations have the same opportunity to turn marketing spin around 'trustworthiness' into action. We have had conversations with the ONDC and other organisations and we are hopeful that our ideas will manifest in future templates, guidance and contracts. This approach is very promising — for both organisations and data subjects —

[318] See above n 279 and accompanying text.

[319] See, eg, *Privacy Policy Template* (Template) <https://www.pwc.com.au/about-us/social-impact/Privacy-Policy-Template.docx.pdf>, archived at <https://perma.cc/N9S9-EWX7>; Woolworths Group, *Woolworths Group Privacy Policy* (Policy, 9 July 2024) <https://www.woolworthsgroup.com.au/content/dam/wwg/privacy/Woolworths_Group_Privacy_Policy_20240709.pdf>, archived at <https://perma.cc/D3XQ-4SK2>; Coles Group, *Privacy Policy* (Policy, August 2024) 2 <https://www.coles.com.au/content/dam/coles/coles-financial-services/insurance/pdf/privacy-policy/Coles%20Group%20Privacy%20Policy%20-%20June%202024.pdf>, archived at <https://perma.cc/WPH2-VGV4>.

[320] See above Part II(B).

[321] See above Parts IV–V.

because it would engender a data sharing culture that acknowledges and values the role of data subjects in the new data economy: a culture that welcomes the adoption of data governance mechanisms to strengthen data literacy and protection.

VII Appendix: List of Reviewed Data Sharing Agreements and Template Agreements

A *Australia*

Table 1: Government Agreements and Templates Reviewed

Body or Jurisdiction	Title of Agreement or Template
Commonwealth; Australian Capital Territory; New South Wales; Northern Territory; Queensland; South Australia; Tasmania; Victoria; Western Australia	Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments[322]
Office of the National Data Commissioner, Australian Government	Data Sharing Agreement[323]
Government of the Australian Capital Territory	Data Sharing Agreement[324]
Department of Customer Service, Government of New South Wales	Data Sharing Agreement Generator User Guide (Prototype V2)[325]
Department of the Premier and Cabinet, Government of South Australia	Data Sharing Agreement between South Australian Government/Non-Government[326]
Government of Victoria	Victorian Public Sector (VPS) Data Sharing Heads of Agreement[327]

[322] *Intergovernmental Agreement* (n 1).
[323] *ONDC Agreement* (n 207).
[324] *ACT Agreement* (n 207).
[325] *NSW Agreement* (n 224).
[326] *SA Agreement* (n 224).
[327] *Vic Agreement* (n 224).

Table 2: Non-Government Agreements and Templates Reviewed

Institution	Title of Agreement or Template
Australian Broadcasting Corporation	Data Sharing Agreement: Australia Talks National Survey 2019[328]
Monash Partners Academic Health Science Centre	Data Sharing Agreement and Principles[329]

B *International*

Table 3: Government Agreements and Templates Reviewed

Body or Jurisdiction	Title of Agreement or Template
Centers for Medicare and Medicaid Services, United States Department of Health and Human Services	Sample Interagency Data-Sharing Agreement[330]
NHSX, United Kingdom	Template Data Sharing Agreement[331]
Information Commissioner's Office, United Kingdom	Data Sharing Code of Practice[332]

328 *ABC Agreement* (n 227).

329 *Monash Partners Agreement* (n 229).

330 Centers for Medicare and Medicaid Services, *Sample Interagency Data-Sharing Agreement* (Agreement) <https://jointlearningnetwork.org/wp-content/uploads/2022/01/US-CDC-Sample-Data-Sharing-Agreement.doc.pdf>, archived at <https://perma.cc/X9NY-6657>.

331 NHSX, *Template Data Sharing Agreement* (Agreement) <https://transform.england.nhs.uk/media/documents/Template_Data_Sharing_Agreement_-12April21_-_FINAL.odt>, archived at <https://perma.cc/G5RG-UD5Z>.

332 *UK Agreement* (n 1).

Body or Jurisdiction	Title of Agreement or Template
Inland Revenue, New Zealand Government; Department of Internal Affairs, New Zealand Government	Information Sharing Agreement between Inland Revenue and Department of Internal Affairs[333]
Office of Superintendent of Public Instruction, State of Washington (US)	Agreement between Requestor and the Office of Superintendent of Public Instruction to Authorize the Release and Use of Identifiable Student-Level Data[334]
World Food Programme, United Nations	Data Sharing Agreement[335]

Table 4: Non-Government Agreements and Templates Reviewed

Institution	Title of Agreement or Template
Council of Large Public Housing Authorities	Aligning Education and Housing: Data Sharing Agreement Template[336]
Facebook	Research Data Agreement[337]
GDPR.EU	Data Processing Agreement[338]

[333] Inland Revenue (NZ) and Department of Internal Affairs (NZ), *Information Sharing Agreement between Inland Revenue and Department of Internal Affairs* (Agreement, April 2018) <https://www.ird.govt.nz/-/media/project/ir/home/documents/about-us/publications/approved-information-sharing-agreements/information-sharing-agreement-between-inland-revenue-and-department-of-internal-affairs/2018.pdf?modified=20200605005045&modified=20200605005045>, archived at <https://perma.cc/EY52-JCXL>.

[334] *US Office of Superintendent Agreement* (n 261).

[335] *Data Sharing Agreement* (Agreement) <https://reliefweb.int/report/iraq/data-sharing-agreement-template>, archived at <https://perma.cc/NF6H-VXSQ>.

[336] *Council of Housing Authorities Agreement* (n 262).

[337] *Facebook Research Agreement* (n 265).

[338] *Data Processing Agreement* (n 230).

Institution	Title of Agreement or Template
Google Cloud	Cloud Data Processing Addendum (Customers)[339]
Komatsu Europe International NV	Customer Personal Data Sharing Agreement[340]
Meta	Data Processing Terms[341]
Mimecast	Data Processing Addendum[342]
University College London	Data Sharing Agreement[343]
X (formerly Twitter)	X Controller-to-Controller (Outbound) Data Protection Addendum[344]

[339] 'Cloud Data Processing Addendum (Customers)', *Google Cloud* (Web Page, 4 August 2024) <https://cloud.google.com/terms/data-processing-addendum>, archived at <https://perma.cc/9984-WV64>.

[340] *Customer Personal Data Sharing Agreement* (Agreement) <https://www.komatsu.eu/-/media/projects/komatsu/komtrax-legal-documents/komtrax_customer-personal-data-sharing-agreement.ashx?v=0dc7d3fe1f6445e49d78b4df7faf6220&rev=652adef42ea74b229ba7b8727fd002f4&hash=1C8C869D70EA0465F4969E9F143075A4>, archived at <https://perma.cc/5PKV-S2DG>.

[341] 'Data Processing Terms' (n 264).

[342] Mimecast, *Data Processing Addendum* (Addendum, November 2023) <https://assets.mimecast.com/api/public/content/5caba73b14e843b6b585f5b532208af8>, archived at <https://perma.cc/8SX4-672X>.

[343] University College London, *Data Sharing Agreement* (Agreement) <https://www.ucl.ac.uk/data-protection/sites/data-protection/files/data-sharing-agreement.docx>, archived at <https://perma.cc/K6V3-2QNS>.

[344] 'X Agreement' (n 260).