22 June 2022

Australian Government Department of Home Affairs
Via webform: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security/submissions-national-data-security-action-plan

Submission on National Data Security Action Plan Discussion Paper

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **UNSW Institute for Cyber Security** ('IFCYBER') is a multidisciplinary Institute which focuses on research, education, innovation and commercialisation that has 'real world impact'. The Institute has over 60 members across each of our faculties. We are ambitious (achieving international impact), scholarly, collaborative and inclusive (acknowledging that cyber security is a new and developing field and seeking opportunities to broaden our understandings of the field by welcoming a broad range of disciplines), entrepreneurial (seeking opportunities to empower academics to be creative), diverse (embracing multidisciplinary and working as thought leaders), and generous and supportive (helping to develop and mentor early career academics, recognising vulnerable groups in society).

The **UNSW Data Science Hub** ('uDASH') focuses on solving complex, real-world challenges. The team at uDASH comprises over 90 data scientists from across UNSW psychology, medicine, physics, law, mathematics, education, business, marketing and economics. uDASH exists to see meaning and patterns where others see bits and bytes of information. More details of uDASH can be found at https://www.unsw.edu.au/research/udash.

We are happy to discuss this submission further with the policy team, including by organising a policy roundtable with us and other academics.

About this Submission

We are grateful for the opportunity to make a submission on the Discussion Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public. We have attempted to organise the submission around the questions posed. This does not always align easily as many of the questions are addressed to 'businesses' as opposed to academic commentators. We also make some points that do not easily align with the questions posed, so we start with some comments on the nature of 'data' and end with some specific issues that are relevant only in particular sectors, centred on the financial sector.

Our main points relate to:

- The nature of data and the need for careful use of terms such as "own" when applied to data;
- The challenge of complexity in the legal and regulatory landscape for data security, pointing to existing and ongoing work that maps out aspects of this;
- The benefits of international harmonisation, both generally and in the specific context of financial services and payment systems;
- References to our work on supply chains and cyber security and our work on the complexity of regulation in the context of provision of cloud services;
- The (limited) relevance of size of organisations;
- Some limiting factors that prevent Australian industry and businesses from effectively implementing an enhanced data security regime;
- The need for accountability to focus not only on data breaches but also resilience in responding to data breaches;
- Specific issues in the context of financial services and also the consumer data right regime.

Framing issue – the nature of data

The nature of data, and the appropriate terminology for it, is a vexed question. In many places throughout the discussion paper, data is described as an "asset". We assume that term is used to highlight that it has value, which is fine.

However, data is not necessarily a "thing" under Australian law. Indeed, a wide variety of Australian case law, including from the High Court, confirms that information itself is not property.[1] This renders problematic terms such as "ownership" in relation to data (see eg p 13 of the Discussion Paper).

The following can be the object of property rights in Australia:

- physical media on which data is stored;
- copyright in literary works, artistic works, etc (which will sometimes be the case for data, but not always);
- contractual rights, including a right correlated to an obligation to keep a secret;
- equitable rights, including a right correlated to an equitable obligation of confidence.

There are better words that can be used to describe the relationship between an entity and information than "ownership", which may confuse those familiar with the use of that term in the context of property. For example, the term "controller" can be used or else, following the *Data Availability and Transparency Act*, a term such as "custodian".

Responses to select questions

1. What do you consider are some of the international barriers to data security uplift?

The legal and regulatory framework across Australia is complex. Various factors contribute to this including different laws in different jurisdictions, additional non-legal requirements in the context of

[1] For a fuller discussion of this issue, see Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion', (2020) 43 *University of New South Wales Law Journal* 615 - 641, https://search.informit.org/doi/10.3316/agispt.20200710033134.

government procurement, and lack of consistency and redundancy in terminology.[2] We are currently doing work on the Australian regulatory environment for cloud computing service providers. Even though our focus is on cyber security regulation of the cloud sector, we have identified multiple, intersecting, sector-specific and cross-sectoral regulatory frameworks that impact the delivery of cloud services in Australia. These include international standards that are regularly referred to in Australian regulatory materials about cyber security. We are happy to share the results of that analysis when it is complete.

The challenge is not confined to inconsistencies and complexities within Australia – there is no single internationally accepted data security framework. In addition, foreign laws imposing data security obligations may apply extraterritorially to Australian firms – as demonstrated by Article 3 of the GDPR.[3] As a result, some issues could be resolved more efficiently through international coordination.

We believe that businesses, consumers and regulators may benefit from international legal harmonisation and standardisation of supervisory expectations regarding data security.[4] This can be helpful for a number of reasons. First, a coordinated international response is able to address more efficiently the cross-border nature of cyber threats, which 'requires a high degree of alignment of national regulatory and supervisory requirements and expectations'.[5] Second, legal harmonisation can help to deal with existing (and potential) overlaps in data security regulation. Furthermore, harmonisation can provide useful guidance for overseas legislatures and regulators lacking data security expertise – thereby helping to increase the overall level of data security on a regional (APAC) and global scale. This is important given that, in our experience, there is a considerable dearth in data security expertise across developing and least developed economies.

We anticipate that demand for international harmonisation of data security frameworks will be different across various sectors of the economy. Later in this submission, as an example, we focus on how the financial services sector might benefit from such harmonisation in the short to medium term.

8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

The main challenges relate to the changing technology landscape. This includes increasing use of AI, which both increases the impact of attacks and makes new kinds of attacks possible.

---

[2] Bennett Moses, above n 1.

[3] Regulation (EU) 2016/679 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) (GDPR) (OJ L 119/1) Article 3.

[4] For a detailed analysis of the benefits and challenges of legal harmonisation in this area, see Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) *Uniform Law Review* 125-167 <https://doi.org/10.1093/ulr/unaa006>.

[5] European Commission, 'FinTech Action Plan: For a More Competitive and Innovative European Financial Sector' (2018) 15 <https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF>.

11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?

Through the Cyber Security Co-operative Research Centre, the UNSW Allens Hub has done work with the Department of Home Affairs on a brochure to inform small and medium enterprises in the supply chain for critical infrastructure about obligations and opportunities following changes in critical infrastructure laws. While this brochure has not yet been distributed, it provides one example of Government helping organisations manage supply chain risk.

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).

We agree that there should be overarching guidance on securing data, and that all businesses should be aware of best security practices and implementation issues. We recognise that there may be a need for more tailored guidance in relation to businesses of different sizes and natures.

We appreciate that it may not always be appropriate to assume that a firm's size reflects its level of data security or cyber resilience, as some small companies may implement highly sophisticated data protection tools and methods. Nonetheless, smaller firms (in general) are more likely to lack relevant expertise and are often viewed as the 'weakest link'[6] in data security that requires more specific regulatory guidance and other forms of assistance. Among other things, a firm's size can influence (i) how it chooses to address data security challenges, (ii) its ability to respond to those challenges and, consequently, (iii) the relevance of certain risk factors.

We believe that guidance on securing data should not be based *solely* on a size threshold. Rather than simply elaborating in greater detail what a principles-based approach entails for smaller firms (which is helpful but insufficient), it should seek to address the *specific challenges* identified in (i)-(iii) above. For example, while outsourcing of the data security function could be an attractive solution for smaller firms due to its convenience (i), it may as well become a source of vulnerability: less sophisticated companies may not have the resources to analyse the programming code used by outsourcing providers for vulnerabilities (including back doors) or negotiate appropriate contractual terms with software vendors (ii). This may lead to information asymmetry between small firms and data security service providers, as well as a lack of effective control over the operations of such service providers (iii). For this reason, it would be helpful to consider the international practices in data or cyber security licensing (eg in Singapore and the EU), which Australia's 2020 Cyber Security Strategy has identified as an area for further research 'in the medium to longer term'.[7] Licensable activities of relevance to smaller firms may include, for example, penetration testing services or managed security operations centre (SOC) monitoring services (as defined in the Second Schedule of Singapore's *Cybersecurity Act 2018*).

13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

There are limiting factors that prevent Australian industry and businesses from effectively implementing an enhanced data security regime. These include a lack of understanding particularly in relation to implementation, unclear expectations, and staying up to date.

[6] Australian Government, 'Privacy Act Review Discussion Paper' (October 2021) 42.

[7] Australian Government, 'Australia's Cyber Security Strategy 2020' (2020) 33.

Lack of understanding

One major hurdle is the lack of understanding of how to use technology to protect data. It is simple to state that to protect against the harms associated with data breach, data should be sufficiently anonymised or else encrypted. However, incorrectly implementing these technologies can be catastrophic. For example, data that has gone through an insufficient de-identification process can still be re-identified. Educating industry and businesses to not only understand and implement the best practices, but also perform regular security audits will be helpful.

Unclear expectations

The cyber security legal framework in Australia is complicated, with at least 51 Commonwealth, State and Territory laws.[8] It includes rules that are cross-sectoral (eg the *Privacy Act 1988* (Cth), the *Security of Critical Infrastructure Act 2018* (Cth), the Consumer Data Right framework), sectoral (eg the obligations of Australian Financial Services Licence (AFSL) holders under s 912A(1)(h) of the *Corporations Act 2001* (Cth) to have adequate risk management systems) and sub-sectoral (eg APRA's Prudential Standard CPS 234). There is also international guidance, recommendations and standards.[9]

Despite the coexistence of multiple (and occasionally overlapping) frameworks, the level of expectation often remains unclear – even in the most regulated sectors, like financial services. This can be illustrated by ASIC's first-ever litigation against an AFSL holder (RI Advice Group Pty Ltd, '**RI Advice**') over poor cyber security controls that was eventually settled, with the final judgment issued in May 2022.[10] These proceedings revealed the lack of a clear legal standard prescribed by s 912A(1)(a) (which requires AFS licensees to 'do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly'). Abstract notions like 'efficiency' integrated into this provision generate uncertainty and confusion, making both businesses and regulators waste time and money debating about the proper standard of behaviour (such as the test of 'public expectation' proposed by ASIC and rejected by RI Advice).

The complexity of attempts to distil clear expectations regarding data security was acknowledged by the court, which concluded that cyber risk management 'is not an area where the relevant standard is to be assessed by reference to public expectation'[11] and further noted:

> 'Cyber risks, an adequate response to such risks and building cyber-resilience requires appropriate assessment of the risks faced by a business in respect of its operations and IT environment. Cyber risk management is a highly technical area of expertise. The assessment of the adequacy of any particular set of cyber risk management systems requires the technical expertise of a relevantly skilled person.'[12]

---

[8] Australian Government, 'Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views' (2021) 12.

[9] On international guidance, recommendations and standards, see Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) *Uniform Law Review*125 <https://doi.org/10.1093/ulr/unaa006>.

[10] *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496.

[11] Ibid [47].

[12] Ibid [46].

The court's reasonable conclusion that in these circumstances 'the adequacy of risk management must be informed by people with technical expertise in the area'[13] suggests that the existing legal framework can be too vague (almost ethereal) in the context of data security – as the required standard of behaviour is effectively determined *ex post*, rather than *ex ante*. This lack of certainty reduces predictability, which is necessary in economic relations. In the absence of such certainty, as the above case demonstrates, parties are likely to resort to battles of expert opinions. Ironically, even this may not be enough, as the court ultimately ordered RI Advice to engage a third party expert to 'identify what, if any, further documentation and controls in respect of cybersecurity and cyber resilience are necessary for RI Advice to implement to adequately manage risk in respect of cybersecurity and cyber resilience'.[14]

The above case illustrates well the challenges of interpreting and enforcing vague data security standards and highlights the importance of establishing clear data security expectations. It also strongly suggests that relying on courts to develop the jurisprudence and add the much-needed clarity in such a technical area may well be futile. Therefore, in our view, an articulation of required standards of conduct (whether or not by reference to existing international or domestic standards) should be developed as a matter of urgency – to give both businesses and regulators the legal certainty to enable efficient compliance and minimise the costs of enforcement.

In conclusion, it is worth noting that the above issues are not limited to finance and are likely to be relevant in other sectors of Australia's economy with vague data security standards.

Keeping data security laws up to date

A recurring challenge in designing data security frameworks is the need to keep the applicable rules up to date in the light of emerging technologies and increasing sophistication of attackers. Obsolete laws can discourage implementation of an *enhanced* data security regime.

In response to this challenge, some overseas data security laws have incorporated references to best practices and the latest technological developments. Some of them contain provisions considering the *current level of technology*. For example, under the GDPR in the European Union, technical and organisational measures to ensure security of data processing must be implemented 'taking into account the *state of the art*'.[15] Others implement provisions focused on *current best practices*. For example, the Cyber Resilience Oversight Expectations for Financial Market Infrastructures of the European Central Bank expect financial market infrastructures to 'employ *best practices* when implementing changes' at the basic ('evolving') level of cyber resilience expectation[16] and to set up change management process based on 'well-established and industry-recognised standards and *best practices*' at the higher ('advancing') level.[17]

---

[13] Ibid [47].

[14] Ibid [3].

[15] Regulation (EU) 2016/679 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) (GDPR) (OJ L 119/1) Article 32(1).

[16] European Central Bank, Cyber Resilience Oversight Expectations for Financial Market Infrastructures' (2018) <https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf> s 2.3.2.1(44).

[17] Ibid s 2.3.2.1(52).

Both groups aim to facilitate the highest possible (at the time) level of preparedness and deliberately use discreet language, generally encouraging the use of up-to-date techniques, but not always making them mandatory. Yet, the scope of the two approaches is slightly different. The first group is concerned purely with the level of technology—that is, *what is technically possible* at the time. The second group is more reactive, as it is based on the *current level of industry practices*, which may or may not adequately tackle data security issues at the current level of technology. As a result, the former group is likely aimed at more sophisticated firms with sufficient resources to analyse the level of technological advancement in the entire sector.[18]

We think it is important that the data security regulatory framework in Australia remains sufficiently flexible to keep pace with the current best practices (which will inevitably change over time).

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

We agree that there should be enhanced accountability mechanisms for government agencies and industry in the event of data breaches. Agencies that implement security by design should be rewarded and those who do not should be required to make the necessary adjustments. Security audits can also result in improved public trust. However, the issue is not only about data breaches but also organisational resilience.

The desirability of enhanced accountability mechanisms that focus solely on data breaches depends on the objectives of the data security framework. Is there an underlying expectation that principles-based laws, if applied correctly, will make it possible to *prevent all* data breaches? We emphasise that cyber threats to data security demand a different attitude 'based on the realistic assumption that not all attacks can be prevented',[19] which implies greater emphasis on *responding* to breaches (including by providing compensation to affected persons) rather than attempting to build impenetrable cyber fortresses. The inevitability of data security breaches has been acknowledged even in the most sophisticated industries in terms of data protection, like finance. For example, the severity and imminence of cyber risks in our banking system is emphasised by the Reserve Bank of Australia (RBA), which concluded in its October 2021 Financial Stability Review that 'a significant cyber event that has the potential for systemic implications is at some point inevitable'.[20] Thus accountability needs to extend beyond data breaches to organisational cyber security and resilience.

Sector-specific issues

International harmonisation

Above, we looked broadly at the benefits of international harmonisation; here we focus specifically on the financial services sector. In particular, we consider the emergence of innovative payment instruments that call for a coordinated international response such as global stablecoins (GSCs) including Diem or Celo and so-called central bank digital currencies (CBDCs)

[18] For further analysis of this issue see Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) *Uniform Law Review* 158-160 <https://doi.org/10.1093/ulr/unaa006>.

[19] Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) *Uniform Law Review* 128.

[20] Reserve Bank of Australia, 'Financial Stability Review' (October 2021) 38.

including e-CNY developed by the People's Bank of China. It is also possible that new digital forms of the Australian dollar will be issued in the future as a response to the e-CNY and similar initiatives from other major economies.

Data security risks associated with GSCs and CBDCs are more significant due to the increased data concentration that characterises these initiatives. Global stablecoins are, by definition, offered on a wide basis, potentially with systemic implications. CBDCs can be designed to cover a large customer user base (which could be economy-wide, regional or even global). This can make GSC and CBDC platforms attractive targets for cyber attackers, with possible major systemic consequences resulting from successful breaches.

The design of GSCs and CBDCs will determine the magnitude of associated data security risks. For example, one important factor is the number and types of end-users with access to new currency types: 'Defending against cyber attacks will be made more difficult as the number of endpoints in a general purpose CBDC system will be significantly larger than those of current wholesale central bank systems.'[21]

The rollout of CBDCs abroad raises important questions for the Australian Government. Will it help to promote the safety of personal data of Australians if an overseas retail CBDC (such as e-CNY) becomes widely available to Australian citizens? Will any protective measures be implemented – and if so, which ones? It is highly probable that major economies (like China or the United States) would use CBDCs not only to improve their *domestic* payment networks, but also to project their economic power to other countries by controlling vast amounts of valuable transactional data about the Australian economy and personal data of Australians using such CBDCs. Major foreign economies have powerful tools to force Australian businesses to comply with their laws – as exemplified by the unprecedented extraterritorial reach of the US *Foreign Account Tax Compliance Act* (FATCA), which some scholars dubbed 'by far the most egregious example of extraterritorial overreach in history'.[22]

As major overseas CBDCs become widely available to Australian firms and individuals, large amounts of valuable data (including payment transactions information) will be controlled by foreign businesses and accessed by foreign regulators. Just like with FATCA, Australia may be forced to negotiate some form of international (bilateral or multilateral) legal regime in response. However, to have any leverage in those negotiations, Australia likely needs its own CBDC in the first place. These considerations should be at the centre of any discussions about the prospects of a retail CBDC in Australia – including the upcoming joint study by the Reserve Bank of Australia and the Treasury.[23]

Another international barrier that could be addressed via international legal harmonisation is the duplication of regulatory requirements for Australian firms operating on a cross-border basis. For example, cyber-reporting requirements and cyber threat intelligence-led penetration testing schemes (such as CBEST in the UK, TIBER in the EU, iCAST in Hong Kong, and the CORIE framework in Australia) may generate inefficiencies through multiplication of regulatory obligations relating to essentially the same activities (such as reporting of cyber incidents) or through the need to conduct resource-intensive adversarial attack simulation exercises managed by regulators in different countries.

---

[21] Bank for International Settlements, 'Central Bank Digital Currencies: Foundational Principles and Core Features' (Report No 1, 2020) 5 <https://www.bis.org/publ/othp33.pdf>.

[22] Bruce W Bean and Abbey L Wright, 'The US Foreign Account Tax Compliance Act: American Legal Imperialism?' (2015) 21(2) *ILSA Journal of International and Comparative Law* 333, 367.

[23] Australian Government, 'Transforming Australia's Payments System' (December 2021) 13.

While the financial sector may benefit the most from international harmonisation of cybersecurity regulations in the immediate future, it is worth identifying other sectors of the economy that may equally benefit from harmonisation or initiatives that could help improve cybersecurity on an economy-wide basis. One area to consider is harmonisation of licensing regimes for data or cyber security service providers.

Finally, we note that despite its ability to overcome certain international barriers to data security uplift, international legal harmonisation in this area is subject to several limitations. These include weak international enforcement and the proliferation of unilateral sanctions in international relations that have significantly diminished the role of international rules in recent years. Furthermore, certain forms of international cooperation may leave Australia vulnerable – eg if cyber intelligence information ends up being shared with an adversary state or is intercepted by malicious actors. These challenges need to be carefully considered to reap the benefits of an internationally coordinated approach without jeopardising Australia's national data security.

Improving public trust through the Consumer Data Right ('trusted advisers' framework)

The recent expansion of the consumer data right (CDR) framework via the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* has introduced a significant change to the CDR data sharing model.[24] More specifically, the revised CDR Rules have introduced a new concept of 'trusted advisers' and authorised disclosure of CDR data to trusted advisers *without requiring them to obtain CDR accreditation*. According to the revised CDR Rules, trusted advisers include providers of certain specialist services, in particular:

- **qualified accountants** within the meaning of the *Corporations Act 2001* (Cth);
- persons who are admitted to the **legal profession**;
- registered **tax agents**, **BAS agents** and **tax (financial) advisers** within the meaning of the *Tax Agent Services Act 2009* (Cth);
- **financial counselling agencies** within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*;
- 'relevant providers' within the meaning of the *Corporations Act 2001* (Cth) (ie individuals authorised to provide **personal advice to retail clients** in relation to relevant financial products), with certain exceptions; and
- **mortgage brokers** within the meaning of the *National Consumer Credit Protection Act 2009* (Cth).[25]

The above professionals are not subject to bespoke data security controls envisaged by the CDR framework, which targets mainly accredited data recipients (ADRs). In short, in a relationship between the disclosing entity (an ADR) and the trusted adviser acting as the recipient of disclosed CDR data, the relevant protections apply to the former – but not to the latter. The Explanatory Statement to the relevant amendments states that 'disclosure of the CDR data from an accredited data recipient to a trusted adviser is covered by the information security controls in Schedule 2 to the CDR Rules'[26] – however in practice the only relevant control implied in this case is the obligation

[24] For a detailed analysis of the 'trusted adviser' framework within the CDR, see Anton Didenko, *Implications of the Consumer Data Right Framework for Trusted Advisers* (Report for CPA Australia, March 2022) <https://ssrn.com/abstract=4065189>.

[25] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 1.10C(2) ('CDR Rules').

[26] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021: Explanatory Statement 20.

of the ADR to protect CDR data in transit e*n route to the trusted adviser*.[27] In other words, these protections – in the context of CDR data transfers from ADRs to trusted advisers – apply to data *in transit*, rather than data *at rest* (once such data have reached the recipient).

Furthermore, the CDR framework provisions concerning trusted advisers do not establish an unequal relationship (as observed, for example, in the case of sponsored accreditation): ADRs are not responsible for the actions or information systems of trusted advisers. The latter only act as CDR data recipients and are subject to their own information security rules (which may or may not be as strict as those found in Schedule 2 of the CDR Rules). In other words, instead of establishing a single data security framework for different recipients of CDR data, the reforms have made possible co-existence of two parallel regimes (with different requirements for data security): one for ADRs and one for trusted advisers.

Under the revised CDR framework, trusted advisers may end up being the 'weakest link' in the chain of transfers of valuable CDR data. Whether this risk will materialise will depend on the relevant duties applicable to different classes of trusted advisers outside the CDR framework (since the latter is carefully drafted to avoid direct regulation of trusted advisers). In this context, the data security capability and obligations of trusted advisers become particularly important.

Considering that trusted advisers are not subject to the accreditation requirements of the CDR framework, safeguarding CDR data disclosed to this group of professional service providers becomes crucial. Because of this, we argued in our earlier submission to the Australian Attorney-General's Department on the Privacy Act Review Discussion Paper (October 2021)[28] that the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* should serve as a catalyst for the immediate adjustment or complete elimination of the small business exemption under the *Privacy Act 1988* (Cth). If a complete abolition of the small business exemption is not feasible, we suggested that all classes of trusted advisers, as defined by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*, should not enjoy any exemptions from the application of the *Privacy Act 1988* (Cth).

However, revision of the *Privacy Act 1988* (Cth) is only one step towards greater data security of trusted advisers – a matter that should be a regulatory priority. As the amended CDR Rules are already in place, we stress that the floodgates have been opened for the CDR data to be channelled from the highly regulated CDR environment to entities that are not subject to CDR data security controls. This is particularly important if one accepts the argument of some commentators, like the Australian Privacy Foundation, that '[d]ata breaches are a near certainty' and the proper question 'is not if but when'.[29]

---

[27] See CDR Rules, Schedule 2, Part 2, r 2.2.

[28] UNSW Allens Hub, Deakin University Centre for Cyber Security Research and Innovation and IEEE Society on Social Implications of Technology, 'Submission on the Privacy Act Review Discussion Paper (October 2021)' (Submission, 10 January 2022) <https://www.allenshub.unsw.edu.au/sites/default/files/inline-files/20220110%20Submission%20to%20AGD%20regarding%20Privacy%20Act%20Review%20Discussion%20Paper.pdf>.

[29] Australian Privacy Foundation, 'Submission to the Issues Paper: Inquiry into the Future Directions of the Consumer Data Right' (6 May 2020) 2 <https://treasury.gov.au/sites/default/files/2020-07/australian-privacy-foundation.pdf>. For a detailed analysis regarding cyber security implications in finance, see Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond' (2020) 25(1) *Uniform Law Review* 125.

Improving public trust through the retail CBDC design

Despite the RBA's earlier conclusion that there was no *immediate* need for a retail CBDC in Australia,[30] preparations for the possible rollout of a CBDC in the future are well underway. In December 2021, the Reserve Bank of Australia completed its first project to develop a *wholesale* CBDC proof-of-concept (Project Atom).[31] In March 2022, the central bank published the results of Project Dunbar (a collaboration with the Bank for International Settlements Innovation Hub Singapore Centre, Bank Negara Malaysia, the Monetary Authority of Singapore and the South African Reserve Bank), which explored how a common platform for *multiple* CBDCs could facilitate cross-border payments.[32] The Australian Government has agreed, in principle, with the recommendation of the Senate Select Committee on Australia as a Technology and Financial Centre[33] that the Treasury should lead a policy review of the viability of a *retail* CBDC in Australia: such review is expected to be conducted (jointly by the Treasury and the RBA) by the end of 2022.[34]

Adoption of CBDCs by major economies like China (which has been testing its e-CNY for several years) and the United States (which has recently embarked on a major study of the feasibility and implications of a CBDC authorised by the President's Executive Order)[35] may well hasten the global rollout of CBDCs and change the RBA's current stance on the desirability of a retail CBDC in Australia. The launch of a retail CBDC in Australia (ie, a CBDC that is widely available to all Australians) will generate significant data security risks that must be addressed to promote public trust in this new digital form of national currency – to ensure that it is both *trusted* and *trustworthy*.

Crucially, a retail CBDC may turn the RBA into a major holder of personal information and other kinds of valuable payment and balance data for the entire economy. Potential data security risks in this case will be significant for several reasons.

First, data concentration in the computer systems of the RBA will make cyber attacks on the central bank particularly lucrative, promising substantial and immediate payoffs. Despite the RBA's strong record of data security so far, history shows that central banks are certainly not immune to cyber threats, as demonstrated by the many cyber breaches of central banks (including the US Federal Reserve and the European Central Bank,[36] and most recently in 2021 – the Reserve Bank of New Zealand).[37]

Second, while data security risks of Australia's retail CBDC will depend on the design features of the new currency which are yet to be determined (eg, the method of distribution to end-users, integration into existing payments frameworks), a fundamental underlying concern is whether the

[30] RBA, 'Submission to the Senate Select Committee on Financial Technology and Regulatory Technology' (December 2019).

[31] RBA, 'Project Atom: Exploring Wholesale CBDC for Syndicated Lending' (December 2021).

[32] BIS Innovation Hub et al, 'Project Dunbar: International Settlements Using Multi-CBDCs' (March 2022).

[33] The Senate, 'Select Committee on Australia as a Technology and Financial Centre' (Final Report, October 2021) recommendation 8.

[34] Australian Government, 'Transforming Australia's Payments System' (December 2021) 13.

[35] Joseph R Biden Jr, *Executive Order on Ensuring Responsible Development of Digital Assets* (9 March 2022).

[36] Antoine Bouveret, 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment' (IMF Working Paper, 2018) 8-9.

[37] CISCO, 'Securing Australia's Critical Infrastructure' (2021) 11.

development of the CBDC platform is conducted internally by the regulators or Government-controlled entities or ends up being outsourced to a (domestic or foreign) third party. There may be meaningful advantages in outsourcing (eg in terms of expertise some external developers may offer) – but this comes with substantial data security risks (including zero-day vulnerabilities) caused by inadequate coding, undocumented features or even developer's malicious intent.

Alarmingly, in our experience in private banking practice, software developers/vendors generally seek to insulate themselves from accountability using contractual terms. In academic literature, this phenomenon has been referred to as an unusual 'legal cocoon' of software vendors and developers: according to one study based on examination of hundreds of software licence agreements, the problem is not limited to software developed for consumers and is prevalent even in contracts with sophisticated commercial parties.[38] Software can be offered on 'as is' basis (effectively eliminating liability), may come with excluded warranties and with express acknowledgement that it may not be error-free; finally, even where some developer liability remains, it is likely to be capped (eg, to the amount of fees paid for the development of the software).

We appreciate that from the end-user's perspective, the CBDC development process is probably largely irrelevant – provided the CBDC platform remains secure. However, from the operator's (central bank's) perspective, the reputational risks in the event of data security breaches caused by inadequate programming are significant. As a result, the RBA's ability to prevent cyber incidents (and remedy any incidents without delay) will be crucial.

Considering the substantial concerns expressed by Australians about the privacy of their data[39] and the systemic importance of a retail economy-wide CBDC platform, we believe it is important for all outsourcing contractual documentation regarding CBDC development (including the liability and remuneration of the third-party developer) to be made public as long as Australia's CBDC is funded by the public. We also think that Australians should not bear the costs of the CBDC platform's defects – whether caused by the third-party developer's mistakes or ill intent. Given the magnitude of risks associated with the data security of a national CBDC, what kinds of arrangements will be put in place to provide adequate compensation to end users (especially consumers)? The Government's response to these issues will largely define the level of public trust in Australia's own retail CBDC.

Lyria Bennett Moses (UNSW Allens Hub, UNSW IFCYBER, uDASH)

Anton Didenko[40] (UNSW Allens Hub, UNSW IFCYBER)

Yanan Fan (UNSW uDASH)

---

[38] Marian K Riedy and Bartlomiej Hanus, 'It Is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities' (2017) 48 *Loyola University Chicago Law Journal* 1099.

[39] See, eg, Accenture, 'Tech Giants, Online Retailers Face Uphill Battle Pursuing Bank Market Share in Australia, But New "Open Banking" Rules Could Tilt the Landscape, Accenture Research Finds' (Media Release, 25 July 2018) <https://newsroom.accenture.com/news/tech-giants-online-retailers-face-uphill-battle-pursuing-bank-market-share-in-australia-but-new-open-banking-rules-could-tilt-the-landscape-accenture-research-finds.htm>.

[40] The research conducted by Anton Didenko was funded by the Australian Government through the Australian Research Council (project FL200100007 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks'). The views expressed are those of the author and are not necessarily those of the Australian Government or Australian Research Council.

Lesley Land (UNSW Allens Hub)

Susanne Lloyd-Jones (UNSW Allens Hub)

Rob Nicholls (UNSW IFCYBER)

Sushmita Ruj (UNSW IFCYBER)