'KNOW YOUR CUSTOMER' IN THE DIGITAL AGE: CHALLENGES OF PRIVACY, DATA SECURITY AND THE SPEED OF TECHNOLOGICAL DEVELOPMENT

JEANNIE MARIE PATERSON*

CONTENTS

I INTRODUCTION

This article arose from a workshop to 'appraise Australian confiscation and related anti-money laundering laws ("AML") for their effectiveness and compatibility with fundamental rights'. As a variation on that topic, in this article, I consider the interaction between 'know your customer' ('KYC') laws that exist as a part of AML and the statutory regimes with which KYC laws overlap, including those governing privacy, data protection, financial services, digital identity and open banking. My broader theme is regulatory coherence, meaning a concern with the consistency and cohesion of legal obligations.[1] Issues of coherence may arise between statute and common law[2] or the

* Professor, University of Melbourne Law School.

1 See generally Ross Grantham and Darryn Jensen, 'Coherence in the Age of Statutes' (2016) 42(2) *Monash University Law Review* 360; Andrew Fell, 'The concept of coherence in Australian private law' (2018) 41(3) *Melbourne University Law Review* 1160.

2 Elise Bant, 'Statute and Common Law: Interaction and Influence in Light of the Principle of Coherence' (2015) 38(1) *University of New South Wales Law Journal* 367.

provisions of a statute.[3] However, here, I am interested in the interaction between seemingly discrete statutory regimes that nonetheless impose overlapping obligations informed by different objectives.

The interactions I am considering demonstrate a particular kind of regulatory dilemma, or problem of coherence, which is the common inability of interdependent statutory regimes to achieve all of their goals at the same time.[4] In the context of KYC, the dilemma arises because the decision to enact legislation in pursuit of one objective—such as responding to criminal activities through mandatory reporting of suspicious transactions—inevitably impedes the pursuit of other objectives promoted under different legislation, such as protecting privacy and data or encouraging innovation in financial services markets. The evolving use of new technologies may only amplify the problem, as the object and indeed the methods of regulation may themselves be rapidly changing. Moreover, the impact of different statutory obligations and the resulting tensions between regulatory objectives cannot easily be resolved, even by improved legislative design or drafting (although these will assist). It simply may not be possible to achieve all goals of these overlapping statutory regimes at the same time and in the same context. This in turn requires scrutiny of those goals and the efficacy of the legislative interventions seeking to achieve them.

There is considerable debate about the effectiveness of KYC laws, especially as compared to the burden on reporting entities that must comply with the oversight, reporting and monitoring requirements of the regime.[5] Doubts about how effective KYC laws are make it even more pertinent to consider the impact of the laws on other regulatory goals. KYC laws impede individual privacy and raise concerns about government surveillance enabled by private firms tasked with collecting information and monitoring transactions to further government policies. The costs of compliance with KYC laws may stifle innovation or place a disproportionate burden smaller or recent market entrants, working against the interests of the financial sector as a whole.

These issues of regulatory coherence and the weight that should be accorded to KYC objectives have been brought to the fore by a recent suite of relevant regulatory initiatives, which involve (i) extending the application of KYC in the domain of crypto asset intermediary services and professional advisers;[6] (ii) reforming the *Privacy Act 1988*

---

3 Compare, investigating the internal issues of coherence in complex legislation Australian Law Reform Commission, *Legislative Framework for Corporations and Financial Services Regulation: Complexity and Legislative Design* (Background Paper FSL2, October 2021). Cf also Stephen Bottomley, 'Corporate Law, Complexity and Cartography' (2020) 35(2) *Australian Journal of Corporate Law* 142.

4 See also Yesha Yadav and Chris Brummer, 'Fintech and the Innovation Trilemma', (2019) 107(2) *Georgetown Law Journal* 235; Simon Chesterman, 'From Ethics to Law: Why, When, and How to Regulate AI' in David J Gunkel (ed), *Handbook on the Ethics of Artificial Intelligence* (Edward Elgar, forthcoming).

5 See, eg, Charles Littrell, 'Biases in National Anti-Money Laundering Risk Assessments' (Research Paper, 21 January 2022) <https://ssrn.com/abstract=4137532>; Tony Boyd, 'Anti-Money-Laundering is a Joke', *Australian Financial Review* (online, 6 August 2022) <https://www.afr.com/chanticleer/anti-money-laundering-is-a-joke-20220805-p5b7ho>.

6 Australian Government Attorney General's Department, *Modernising Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime* (Consultation Paper, April 2023) ('*Modernising Australia's AML/CTF Regime*').

(Cth) ('*Privacy Act*') to update its application in the digital age;[7] (iii) increasing penalties for data breaches;[8] (iv) applying financial services regulation to crypto and digital asset platforms;[9] (v) growing the capabilities of technology in advancing regulatory oversight; (vi) introducing a legislative framework for digital identity;[10] and (vii) extending the Consumer Data Right in the domain of Open Banking.[11]

Crypto assets—such as cryptocurrencies, non-fungible tokens, and coins[12]—have been linked to criminal activities, including laundering proceeds of crime, criminal transactions, and cyber ransoms.[13] Criminals commonly use crypto assets as a basis for investment scams,[14] and they are a preferred form of payment within a scam.[15] Proposals for applying KYC laws to a broader number of crypto asset intermediary services may cut across one of the key attractions for crypto investors, namely a high degree of anonymity in any transaction.[16] Moreover, the cost burden of complying with newly imposed KYC laws[17] may stifle the growth of innovative FinTech companies in the Australian market,[18] possibly contrary to the aspirations of Open Banking.[19] These consequences may be an acceptable trade-off given the concerns about money laundering, scams and criminal activities utilising crypto assets. Indeed, in Australia, the Commonwealth Government envisages that its proposed KYC reforms will work in conjunction with greater regulatory oversight of crypto assets in the domain of financial

---

7 Australian Government, *Government Response to the Privacy Act Review Report* (2023) ('*Government Response to the Privacy Act Review*').

8 *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth).

9 Commonwealth Treasury, *Regulating Digital Asset Platforms* (Proposal Paper, October 2023) 2 <https://treasury.gov.au/consultation/c2023-427004> ('*Regulating Digital Asset Platforms*').

10 'Your Guide to the Digital ID Legislation and Digital ID Rules', *Australia's Digital ID System* (Web Page, 18 Sept 2023) < https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions> ('*Your Guide to the Digital ID Legislation and Digital ID Rules*'); Explanatory Memorandum, Digital ID Bill 2023 (Cth).

11 Australian Government, *Inquiry into Future Directions for the Consumer Data Right* (Final Report, October 2020) ('*Future Directions*').

12 ASIC, 'Cryptocurrencies: The Risks of Investing in Crypto', *Moneysmart* (Web Page) <https://moneysmart.gov.au/investment-warnings/cryptocurrencies> ('Cryptocurrencies').

13 Alana Maurushat and Dan Halpin, 'Investigation of Cryptocurrency Enabled and Dependent Crimes' in Doron Goldbarsht and Louis de Koker (eds) *Financial Technology and the Law: Combatting Financial Crime* (Springer, 2022) 246–54; Shlomit Wagman, 'Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing' (2022) 14 *Harvard National Security Journal* 87, 89.

14 Commonwealth Treasury, *Token Mapping* (Consultation Paper, February 2023) 5. See ASIC, 'Crypto Scams: Stop and Think to Reduce the Risk of Crypto Scams', *Moneysmart* (Web Page) <https://moneysmart.gov.au/financial-scams/crypto-scams> ('*Token Mapping*').

15 *Token Mapping* (n 14) 5. On scams, generally see ASIC, *Scam Prevention, Detection, and Response by the Four Major Banks* (Report 761, April 2023) ('*Scam Prevention*').

16 See Maurushat and Halpin (n 13) 242–5: distinguishing between crypto-enabled and crypto-dependent crime.

17 Australian Government Attorney-General's Department, 'Anti-Money Laundering and Counter-Terrorism Financing' (Web Page) <https://www.ag.gov.au/crime/anti-money-laundering-and-counter-terrorism-financing> ('Anti-Money Laundering').

18 *Regulating Digital Asset Platforms* (n 9).

19 Cf concerns about compliance burden on lawyers and chief legal officers in AML: Doron Goldbarsht, 'Am I My Corporate's Keeper? Anti-Money Laundering Gatekeeping Opportunities of the Corporate Legal Officer' (2022) 29(3) *International Journal of the Legal Profession* 261.

services,[20] motivated by a concern that crypto assets are often an unreliable and risky investment strategy for inexperienced investors.[21]

Nonetheless, the extended application of KYC laws also highlights the tension of the regime with the regulatory goals of privacy and data protection.[22] For individuals, the notable consequences of KYC laws are more personal information being collected and stored for extended periods. Collecting and storing personal information to allow better scrutiny of money laundering activities may expose individuals to a greater risk of data breaches as bad actors seek to access the troves of data collected by reporting entities. As the recent Optus and Medicare data breaches show, the more data an organisation collects and retains, the greater the potential for public harm from data breaches.[23] These concerns may be amplified by extending KYC obligations to entities that have, at least until now, been less robustly regulated than traditional financial services providers and are potentially less equipped to manage these obligations.

In the face of these ongoing tensions between the objectives of KYC laws, the costs of regulatory compliance and the demands of privacy and data protection, digital technology holds considerable potential attractions. It has frequently been suggested that greater use might be made of technological strategies in identifying and monitoring suspicious transactions, although this itself is not free from risk.[24] Furthermore, the regulatory ambition to both monitor the identity of those engaging in specified currency transactions and respect the demands of privacy and data protection, might be seen almost inevitably to point to the use of digital identity to reduce reliance on individuals repeatedly having to share digital and paper-based copies of critical personal identifiers. Certainly, the Commonwealth Government already operates an accreditation scheme for digital identity service providers who interact with it,[25] and has recently enacted legislation to consolidate and extend this system.[26]

Digital identity schemes aim to give individuals greater control over the personal information they share to establish their identity when dealing with government

---

20 *Token Mapping* (n 14).

21 'Cryptocurrencies' (n 12).

22 Jo Ann Barefoot, 'Regulation Innovation: Using Digital Technology to Protect and Benefit Financial Consumers' (Associate Working Paper Series No 110, Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School 23, 2019).

23 Bianca De Marchi, 'Optus Says it Needed to Keep Identity Data for Six Years. But Did it Really?' *The Conversation* (online, 30 September 2022) <https://theconversation.com/optus-says-it-needed-to-keep-identity-data-for-six-years-but-did-it-really-191498>; James North, Michael do Rozario, James Wallace and Jack Mathews, 'The Optus data breach a timely reminder of your statutory obligations' *Corrs Chambers Westgarth* (Blog Post, 30 September 2022) <https://www.corrs.com.au/insights/the-optus-data-breach-a-timely-reminder-of-your-statutory-cyber-obligations>.

24 'Regtech initiatives and programs', *ASIC* (Web Page) <https://asic.gov.au/for-business/innovation-hub/asic-and-regtech/>.

25 Australian Government, 'Australia's Digital ID System: Trusted Digital Identity Framework (TDIF)', *Australia's Digital ID System* <https://www.digitalidentity.gov.au/tdif> ('Trusted Digital Identity Framework').

26 David McGovern, Leah Farrall and Philip Hamilton, 'Digital Identity (Digital ID) consultation process', *Parliament of Australia* (Web Page, 26 September 2023) <https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/FlagPost/2023/September/Digital_ID_Consultation>.

agencies and businesses, as well as greater security in identity verification.[27] Digital identity schemes further aim to reduce data breach risks through less sharing and retention of personal information. They do this by allowing individuals to verify relevant attributes of their identity digitally instead of by repeatedly sharing identity documents (ie passports, driver's licences or birth certificates).[28] Conceivably, digital identity could reduce the compliance costs of KYC laws. However, digital identity schemes introduce their own concerns. This is because the use of digital identity may be seen as escalating surveillance of individuals by government and private providers of these services.[29]

Learnings from Open Banking might be used to address at least some of these privacy and operational concerns about digital identity schemes. Open Banking also seeks to promote consumer data autonomy by providing a framework for consumers to direct a data holder to provide their banking data to other financial service providers,[30] which should also benefit consumers through greater competition,[31] and new digital banking and investment services.[32] Notably, the Open Banking regime is accompanied by robust privacy protections and is overseen by regulators,[33] which may be a valuable ongoing model for digital identity regulation.[34] Open Banking might also be used to support more streamlined and less data-heavy KYC compliance. However, returning to the regulatory dilemma of incompatible objectives, this use of Open Banking to support KYC law might cut across the aspiration for consumer control over their own data that underlies Open Banking.

This article explores these dilemmas of coherence between overlapping laws with competing regulatory objectives. It begins in Part II by outlining the governing regimes in this field: AML, the *Privacy Act* and financial regulation of crypto assets. Part III considers the proposed reforms under KYC to include a greater range of crypto intermediaries' activities within the regime and the consequential regulatory tensions. Part IV assesses the privacy and cost impacts of these proposals. Part V considers utilising the power of technology in response to the various privacy concerns arising from KYC through greater reliance on so-called RegTech and digital identity verification services. Part VI concludes.

---

27 See, eg, Australian Government, 'Australia's Digital ID System: Privacy and Security', *Australia's Digital ID System* (Web Page) <https://www.digitalidentity.gov.au/privacy-and-security>.

28 See, eg, 'ASIC and MSIC for Government Agencies', *Australian Government Department of Home Affairs* (Web Page) <https://www.auscheck.gov.au/security-card/asic-msic-government-agencies>.

29 Ana Beduschi, 'Digital Identity: Contemporary Challenges for Data Protection, Privacy, and Non-Discrimination Rights' (2019) 6(2) *Big Data & Society* <https://doi.org/10.1177/2053951719855091>.

30 Australian Government, 'How It Works', *Consumer Data Right* (Web Page) <https://www.cdr.gov.au/how-it-works> ('*Consumer Data Right*').

31 *Future Directions* (n 11) 67.

32 Ibid 67–8.

33 'The Consumer Data Right', *ACCC* (Web Page) <https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right>.

34 Greg Kidd, 'Digital Identity: Exploring a Consumer-Centric Identity for Open Banking' in Linda Jeng (ed), *Open Banking* (Oxford University Press, 2022).

II REGULATORY DILEMMAS AND KYC LAWS

A Regulatory dilemmas

Regulating a subject matter that is multifaceted, complex or rapidly changing is difficult. It tends to provoke complex legislation. Complex legislation risks incoherence between provisions, obligations or objectives. It makes compliance difficult. These issues may be amplified with a wider horizon that encompasses not just one statute but a network of legislation with different demands and objectives applying across overlapping domains. Part, though by no means all, of the response to this problem of complexity arising between statutory regimes lies in careful regulatory design. Largely, however, the interaction between overlapping and proximate legislation needs to be resolved as a matter of policy and values, which will mediate the priorities as between the objectives supported by those different regimes.

Yadav and Brummer describe a regulatory trilemma in the field of FinTech; that regulatory interventions seeking to promote certainty, market integrity and innovation are likely only to achieve two out of those three objectives.[35] The problem may be amplified in dealing with new digital technology, which evolve quickly and in highly novel ways. Chesterman refers to the Collingridge dilemma in regulating the outputs and outcomes of new technologies.[36] This dilemma refers to the conundrum that at the early stages of the technology the harms may be unclear, which makes regulation unnecessary or ineffective. Once the technology is more mature and the harms are apparent, regulation may be 'costly and slow'.[37]

KYC, privacy/data protection, and financial services laws are found in different legislation and are overseen by different regulators. The demands of these regimes are not necessarily incompatible. However, the priorities pull in different directions, potentially increasing compliance costs and cyber vulnerabilities. Changing any one element of the governing statutory regime requires careful attention to the whole of the relevant regulatory landscape, not merely the Act in question. Accordingly, the following discussion outlines the general demands of the relevant governing regimes for KYC, privacy and financial services.

B KYC laws

AML regimes aim to prevent and respond to 'serious financial crimes', including money laundering—that is, attempts to conceal the proceeds of money obtained illegally through activities such as drug trafficking, fraud,[38] and terrorist financing.[39] At

---

35 Yadav and Brummer (n 4) 242.

36 Chesterman (n 4) 6. See also discussion in Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology* 1, 8.

37 Ibid.

38 Doron Goldbarsht, 'Am I My Corporate's Keeper? Anti-Money Laundering Gatekeeping Opportunities of the Corporate Legal Officer' (2022) 29(3) *International Journal of the Legal Profession* 261, 263.

39 *Modernising Australia's AML/CTF Regime* (n 6).

the international level, standards for AML are coordinated through the Financial Action Task Force ('FATF'). This intergovernmental body sets international standards for 'anti-money laundering, counter-terrorism financing and countering the financing of proliferation'.[40] Failure to comply with FATF directions risks penalties for reporting entities and constricted access to financial markets for nation states.[41] The relevant instruments 'create a cascading system of supervisory duties, running from state parties to legal entities and from legal entities to associated natural and legal persons'.[42] There is an expectation that member countries will implement the FATF recommendations in a manner tailored to their domestic legal regimes.[43]

FATF recommendations have been implemented in Australia through the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* (Cth). The regime is administered by the Australian Transaction Reports and Analysis Centre.[44] A vital element of the AML regime is KYC. KYC laws impose obligations on designated 'reporting entities' whose businesses centre on money transfers and exchanges, such as financial institutions, the gambling sector, money transfer services, and bullion dealers.[45] Reporting entities must meet specified minimum reporting and monitoring obligations. Thus, KYC laws require reporting entities to collect, verify and retain information about their customers before providing services to them.[46] This includes personal information such as name, date of birth, and address,[47] and verifying documentation.[48] Reporting entities must conduct a risk assessment as to the need for other verifying information.[49]

In addition, reporting entities must have processes to assess the risks of money laundering or terrorism financing in providing the service in question.[50] They must

---

40 'Financial Action Taskforce', *Australian Government Attorney-General's Department* (Web Page) <https://www.ag.gov.au/crime/anti-money-laundering-and-counter-terrorism-financing/financial-action-task-force>.

41 Ronald F Pol 'Anti-money laundering: The world's least effective policy experiment? Together, we can fix it' (2020) 3(1) *Policy Design and Practice* 73, 77.

42 Radha Ivory, 'Due Diligence Debates in International Anti-Corruption and Money Laundering Law: From Content to the Construction of Risk' in Heike Krieger, Anne Peters, and Leonhard Kreuzer (eds), *Due Diligence in the International Legal Order* (Oxford University Press, 2020) 289.

43 'The FATF Recommendations', *Financial Action Task Force* (Web Page, November 2023) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>.

44 'AML/CTF Act', *AUSTRAC* (Web Page) <https://www.austrac.gov.au/business/legislation/amlctf-act>.

45 'Reporting entity', *AUSTRAC* (Web Page) <https://www.austrac.gov.au/glossary/reporting-entity>.

46 'Anti-money laundering', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-legislation/related-legislation/anti-money-laundering>.

47 See *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (Cth) rule 4.2.6 ('*AML/CTF Rules Instrument 2007*').

48 See ibid rule 4.2.7.

49 Ibid rule 4.2.8.

50 'Customer Identification', *AUSTRAC* (Web Page) <https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/customer-identification-know-your-customer-kyc>.

conduct ongoing due diligence, including transaction monitoring.[51] Reporting entities must have processes for identifying suspicious transactions, including for identifying 'unusually large transactions, complex transactions, and unexpected patterns of transactions that don't seem to have a legitimate purpose'.[52] Further, they must report to AUSTRAC certain kinds of transactions,[53] including cash transactions over the reporting threshold (AUD 10,000),[54] international funds transfer reports (transfer of funds in or out of Australia),[55] and 'suspicious matters' that may be related to criminal activity.[56] Reporting entities must keep records of their AML program and due diligence procedures,[57] including records of customer identification and verification, and suspicious matter reports,[58] for a specified period, usually seven years from the transaction date for designated services.[59]

These are complex obligations that include a mix of rule and standard based requirements. A 2016 review*, Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, found that Australia's AML regime was 'overly complex and impedes the ability of regulated entities to understand and comply with their AML/CTF obligations'.[60] A subsequent report, *Modernising Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime* recommended reforms to 'simplify and modernise the operation of the regime'.[61] These changes aimed to assist firms in navigating between AML and other legal regimes, such as financial services and data protection laws. The report also recommended extending the regime's scope to previously unregulated entities, namely 'high risk' professions and digital asset exchanges.[62]

There is a sustained body of criticism of AML/CFT that goes beyond concerns with complexity to question the very effectiveness of the regimes. For example, Neilson, and Sharman have found that sophisticated parties can relatively easily evade

---

51 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 36 ('*AMLCTF Act*'); *AML/CTF Rules Instrument 2007* (n 47) ch 15.

52 'Transaction Monitoring', *AUSTRAC* (Web Page) <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/amlctf-programs/transaction-monitoring>.

53 'Reporting', *AUSTRAC* (Web Page) <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/reporting/reporting-overview>.

54 *AMLCTF Act* (n 51) s 43*; AML/CTF Rules Instrument 2007* (n 47) ch 19.

55 *AMLCTF Act* (n 51) s 44; *AML/CTF Rules Instrument 2007* (n 47) ch 16.

56 *AMLCTF Act* (n 51) s 41; *AML/CTF Rules Instrument 2007* (n 47) ch 18.

57 'Record-Keeping', AUSTRAC (Web Page) <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/record-keeping>.

58 *AMLCTF Act* (n 51) pt 10; *AML/CTF Rules Instrument 2007* (n 47) ch 20.

59 *AMLCTF Act* (n 51) s 107.

60 *Modernising Australia's AML/CTF Regime* (n 6) 3.

61 Ibid. See also Attorney-General's Department, *Paper 5: Broader reforms to simplify, clarify and modernize the regime*, Reforming Australia's anti-money laundering and counter-terrorism financing regime (May 2024) <https://consultations.ag.gov.au/crime/reforming-aml-ctf-financing-regime/user_uploads/paper-5-broader-reforms-to-simplify-clarify-and-modernise-the-regime.pdf>.

62 Ibid.

AML laws, despite KYC requirements.[63] Tsingou argues the achievements of AML in pursuing its goals of responding to financial crime may be modest while the side effects of the regime are to strengthen the position of the largest global financial players.[64] Pol observes there is no "'official" effectiveness measure'[65] or independent verification of the regime[66] and that suggests the forfeiture rates are miniscule compared to value of transactions tainted by organised crime.[67] Levi, Reuter and Halliday argue that without systematic data assessments of how well AML regimes achieve their goals, assessments are based on 'ad hoc, impressionistic or politicised judgments', reducing their legitimacy.[68] Aldridge questions whether money laundering should be considered a serious crime, and certainly whether the issue is so serious as to justify the onerous and extensive reporting requirements including under KYC laws.[69] Although this paper does not assess the effectiveness of AML or KYC, this body of literature supports questioning of the priority given to these laws as compared their cost and impact on innovation in the financial sector, and importantly the overall challenge to privacy, to which we now turn.

III KYC AND PRIVACY, SURVEILLANCE AND DATA PROTECTION

There is an undeniable tension between KYC and privacy/data protection laws.[70] KYC laws undermine privacy rights by requiring reporting entities to collect information about private persons and monitor their transactions. These are not trivial concerns. Privacy is an important if not fundamental right, recognised in domestic legislation and human rights law.[71] Privacy allows the development of individual

---

63 See eg, Daniel Neilson, and Jason Sharman, *Signatures for Sale: How Nominee Services for Shell Companies Are Abused to Conceal Beneficial Owners* (World Bank Group/STAR, 2022). See also Michael Levi, 'Lawyers as money laundering enablers? An evolving and contentious relationship' (2022) 23(2) *Global Crime* 126.

64 E Tsingou, 'Global financial governance and the developing anti-money laundering regime: What lessons for International Political Economy?' (2010) 47 *International Politics* 617, 618 and see esp 628.

65 Pol (n 41) 81.

66 Ibid 82.

67 Ibid 81-83, see also 86, observing 'the current anti-money laundering policy prescription helps authorities intercept about $3 billion of an estimated $3 trillion in criminal funds generated annually (0.1 percent success rate), and costs banks and other businesses more than $300 billion in compliance costs, more than a hundred times the amounts recovered from criminals'.

68 Michael Levi, Peter Reuter, Terence Halliday, 'Can the AML system be evaluated without better data?' (2018) 69(2) *Crime Law and Social Change* 307 and esp 319 discussing suspicious transaction reporting.

69 Peter Alldridge, *What Went Wrong with Money Laundering Law?* (Springer, 2016).

70 Cf Chizu Nakajima, 'The International Pressures on Banks to Disclose Information' in Sandra Booysen and Dora Neo (eds), *Can Banks Still Keep a Secret?* (Cambridge University Press, 2018) 114.

71 See, eg, *Universal Declaration of Human Rights,* GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948) art 12; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

identity[72] and supports other rights such as freedom of expression, movement and speech.[73] Information privacy is a key aspect of privacy and 'critical for building public trust and facilitating participation in public life'.[74] Privacy is not an absolute right and may be constrained in pursuit of other rights, values or justified policy objectives. However, any incursion on privacy rights should generally be necessary and proportionate in achieving those other objectives.[75] Accordingly, the impact of initiatives that intrude on privacy should be assessed and subject to ongoing review,[76] ideally through a publicly visible and contestable process.[77] In this context, doubts about the effectiveness of the KYC laws makes the privacy impact of the regime more precarious than the mantra of 'fighting organised crime might suggest' and certainly justifies ongoing scrutiny of the scope and impact of KYC.

As a corollary to privacy impacts, KYC laws buttress and legitimate extended state surveillance. Surveillance interferes with privacy and has a wider impact by constraining people's enjoyment of their rights.[78] This oversight may seem innocuous, but it gives the state insight into individuals' use of their funds, which may impact the enjoyment of their rights to free expression and political and religious views. Moreover, as Ivory notes, KYC laws represent a delegation of responsibility by the state to private firms to collect information and monitor transactions in pursuit of the state's objectives.[79] Ivory suggests these requirements have a panoptic quality, though, in which 'individuals are encouraged to internalise a sense of being observed, as well to monitor others'.[80] In other words, widespread demands for surveillance as a response to purported threats to the state, such as through money laundering, enshrine and normalise surveillance, while diverting attention from the rights encroached upon by that regime.

---

72 'Managing the Privacy Impacts of a Data Breach', *Office of the Victorian Information Commissioner* (Web Page) <https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/>.

73 'What is Privacy?', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-privacy>.

74 *Government Response to the Privacy Act Review* 5 (n 7).

75 UN Office of the High Commission of Human Rights, *The right to privacy in the digital age* (Report No A/HRC/48/3113, 13 September 2021 [51]. Also *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* ('*General Data Protection Regulation*'), OJ 2016 L119/1, art 35(1).

76 See, eg, Australian Government Attorney-General's Department, *Privacy Act Review* (Report, 2022), 225–6 (Proposal 21.6) ('*Privacy Act Review*'): recommending that:

> The Commonwealth should review all legal provisions that require the retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

See also, in principle, acceptance of this recommendation in *Government Response to the Privacy Act Review* (n 7) 34.

77 Cf Rachelle Bosua, Damian Clifford and Megan Richardson, 'Contact-Tracing Technologies and the Problem of Trust—Framing a Right of Social Dialogue for an Impact Assessment Process in Pandemic Times' (2023) 5(2) *Law, Technology and Humans* 193, 195.

78 The right to privacy in the digital age (n 75).

79 Ivory (n 42) 295.

80 Ivory (n 42) 295.

The privacy impacts of KYC laws are recognised and, to some extent addressed, in Australia. Firms that collect personal information under KYC laws are subject to privacy and data security obligations under the *Privacy Act 1988* (Cth).[81] The *Privacy Act* covers the collection, use, disclosure, quality, and security of personal information by entities of a specific size or activity. The Act is premised on the Australian Privacy Principles ('APPs'), a set of open textured requirements that deal with personal information.[82] The APPs lay down expectations of how personal information, including information collected under KYC requirements, should be handled.[83] These include, for example, a commitment to data minimisation by only collecting personal information reasonably necessary for the collecting entity's functions or activities (APP 3). Individuals need to be provided with notice regarding the collection of personal information and about how their information will be used and disclosed (APP 5). Nonetheless, KYC removes the ability for individuals to choose to transact anonymously (APP 2) or to delete their data (APP 11.2) or even access their personal information (APP 12) in scenarios where there has been a suspicious transaction report.[84] KYC may similarly cut across the premise of Open Banking, which seeks to provide individuals with control over the sharing of personal data within and between financial institutions.[85]

In addition to risks of harm to privacy, KYC laws raise the consequential risk of data breach that arises from extensive personal data collection required under KYC laws. Entities that store large amounts of customer data become a potential target of cyber-attacks,[86] as illustrated by the spate of data breaches in Australia in 2022-23.[87] This exposes individuals to risks that include financial, emotional and reputational harm.[88] Importantly, reporting entities for the purposes of KYC regimes are obliged to protect the security of the information they hold,[89] and to destroy information that is no longer required.[90] Additionally, reporting entities may fall under the scope of the *Security of Critical Infrastructure Act 2018* (Cth), which requires reporting of critical

---

81 *Privacy Act 1988* (Cth) sch 1 ('*Privacy Act*').

82 *Privacy Act* (Cth) sch 1.

83 See further 'Australian Privacy Principles', Office of the Australian Information Commissioner (Web Page) <https://www.oaic.gov.au/privacy/australian-privacy-principles>.

84 Thank you to the reviewers for these examples.

85 See below n 248 ff.

86 See, eg, 'The Broken State of KYC', *Gatenox* (Web Page) <https://gatenox.com/the-broken-state-of-kyc/>.

87 Julian Fell, Georgina Piper and Matt Liddy, 'This is the Most Detailed Portrait Yet of Data Breaches in Australia', *ABC News* (online, 28 March 2023) <https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586>.

88 See 'Managing the Privacy Impacts of a Data Breach', *Office of the Victorian Information Commissioner* (Web Page) <https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/>.

89 Ibid APP 11.

90 Ibid APP 11.

infrastructure to the Cyber and Infrastructure Security Centre and provides powers for that agency and the Government to intervene in the event of a cyber breach.[91]

At the time of writing, the *Privacy Act* is being reviewed to ensure it is fit for purpose in the digital age.[92] One of the most significant proposed reforms in this context relates to the retention of personal information. Under APP 11, entities must take reasonable steps to destroy or de-identify redundant personal information.[93] The period for which an entity may retain information is subject to the retention requirements in the AML Act.[94] Following reports that some firms do not have retention policies,[95] the *Privacy Act Review Report* has recommended providing detailed guidance on reasonable steps for destroying or de-identifying personal information that is no longer required to be held,[96] as well as developing retention policies, having regard to the type, sensitivity, and purpose of the information.[97] These reforms, along with existing *Privacy Act* obligations, will assist in reducing the risk of harm from cyberattacks or other privacy breaches involving KYC information. Nevertheless, the often-repeated mantra is that the only way to protect personal data is not to collect or retain it.[98] Thus, it remains legitimate to assess the merits of any extension of the KYC against the risks to data privacy and other regulatory objectives.

IV KYC AND CRYPTO ASSET INTERMEDIARY REGULATION

The challenge of mediating the competing policy priorities of KYC law and other proximate statutory regimes is further illustrated by recent proposals in Australia to extend KYC laws in their application to crypto asset intermediary services.[99] KYC laws already apply to crypto exchanges.[100] Proposed reforms in Australia, pursuant to FAFT directives, will extend the regulation to a broader pool of crypto asset intermediaries.[101]

---

91 See further *Security of Critical Infrastructure Act 2018* (Cth) <https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure>.

92 *Privacy Act Review* (n 76).

93 *Privacy Act* APP 11.2.

94 Rajaee Rouhani, Ross Phillipson and Jeremy Moller, 'Proposed Changes to Australian Privacy Laws and Their Impact on AML/CTF Compliance', *Norton Rose Fulbright* (Blog Post, April 2023) <https://www.nortonrosefulbright.com/en-au/knowledge/publications/36eaad03/proposed-changes-to-australian-privacy-laws-and-their-impact-on-amlctf-compliance>.

95 North et al (n 23).

96 *Privacy Act Review* (n 76) 13 (Proposal 21.5). Also agreed in the *Government Response to the Privacy Act Review* (n 7) 34.

97 *Privacy Act Review* (n 76) 13 (Proposal 21.7).

98 Tim Briggs, '"The New Asbestos": Does the Optus Hack Spell the End for Paper ID Checks?' *The Sydney Morning Herald* (online, 7 October 2022) <https://www.smh.com.au/technology/the-new-asbestos-does-the-optus-hack-spell-the-end-for-paper-id-checks-20221004-p5bn2h.html>.

99 See Dianna L Kyles, 'Centralised Control Over Decentralised Structures: AML and CTF Regulation of Blockchains and Distributed Ledgers' in Doron Goldbarsht and Louis de Koker (eds) *Financial Technology and the Law: Combatting Financial Crime* (Springer, 2022) 130.

100 *Modernising Australia's AML/CTF Regime* (n 6) 13.

101 Ibid 14.

Before considering these reforms, however, it is necessary to understand crypto assets and the financial services regime that applies to them.

A Crypto assets

Crypto (or digital) assets are 'a cryptographically secured digital representation of value or contractual rights'.[102] The concept covers cryptocurrencies, coins and tokens (including non-fungible tokens).[103] Crypto assets may or may not be backed by physical assets[104] and may be traded using other crypto assets or money.[105] The view has been expressed that, in English law, crypto assets should be recognised as a form of property,[106] and case law has taken this view in dealings with crypto currency.[107] In Australia, in *Australian Securities and Investments Commission v Web3 Ventures Pty Ltd*, Jackman J declined to express a concluded view on this issue.[108]

Transfers of crypto assets are typically executed through smart contracts. Smart contracts consist of performance obligations automated through computer code.[109] Smart contracts operate on or above a distributed ledger platform,[110] such as blockchain.[111] Distributed ledger technology is effectively a database that stores a record of transactions in a way that is (relatively) decentralised, transparent and secure.[112] The transactions recorded on the ledger may be crypto assets or information

---

[102] See, eg, the definition in *Money Laundering and Terrorist Financing (Amendment) Regulations 2019* (UK) SI 2019/1511, Regulation 14(A)(3)(a).

[103] 'Cryptocurrencies' (n 12). See further Kyles (n 99) 136–8.

[104] Jerome Tse, 'Not the Same Token – Treasury Releases its Token Mapping Consultation', *King and Wood Mallesons* (Blog Post, 1 March 2023) <https://www.kwm.com/au/en/insights/latest-thinking/not-by-the-same-token-treasury-releases-its-token-mapping-consultation.html>.

[105] 'Cryptocurrencies' (n 12); The LawTech Delivery Panel, *Legal Statement on Cryptoassets and Smart Contracts (UK Jurisdiction Taskforce)* (Legal Statement, November 2019) 10 ('*Cryptoassets and Smart Contracts*').

[106] *Cryptoassets and Smart Contracts* (n 105) 7. Also, Law Commission, *Digital Assets: Final Report* (Consultation Paper No 256, 28 July 2022). See also *Token Mapping* (n 14) 13. But cf Robert Stevens, 'Crypto is Not Property' (2023) *Law Quarterly Review* (forthcoming).

[107] *Tulip Trading Ltd v Bitcoin Association for BSV* [2023] EWCA Civ 83; [2023] 4 WLR 16 [24].

[108] [2024] FCA 64.

[109] See generally Jenny Cieplak and Simon Leefatt, 'Smart Contracts: A Smart Way to Automate Performance' (2017) 1(2) *Georgetown Law Technology Review* 417.

[110] Cheng Lim, TJ Saw and Calum Sargeant, 'Smart Contracts: Bridging the Gap between Expectation and Reality', *Oxford Business Law Blog* (Blog Post, 11 July 2016) <https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality>. See generally Scott Farrell, Kate Jackson-Mayes and Michael Swinson, '10 Points on Financial Market Smart Contracts', *King and Wood Mallesons* (Blog Post, June 2016) <https://www.kwm.com/au/en/insights/latest-thinking/10-things-you-need-to-know-smart-contracts.html>; Scott Farrell, 'How to Use Humans to Make "Smart Contracts" Truly Smart', *King and Wood Mallesons* (Blog Post, July 2016) ('Making smart contracts truly smart') <https://www.kwm.com/en/au/knowledge/insights/smart-contracts-open-source-model-dna-digital-analogue-human-20160630>.

[111] On the operation of blockchain, see generally Sarah Green and Adam Sanitt, 'Smart Contracts' in Paul S Davies and Magda Raczynska (eds), *Contents of Commercial Contracts: Terms Affecting Freedoms* (Hart, 2020) 191–210.

[112] 'Making smart contracts truly smart' (n 110); Mark Staples, CSIRO Data61, *Risks and opportunities for systems using blockchain and smart contracts* (Technical Report EP175103, May 2017); Alexandra

about property title, payments, movement of goods, or computer code. The ledger is distributed because the records are stored across many computers, or 'nodes'.

The technical features of smart contracts inform their promoted attractions, which are often said to lie in their being autonomous (or self-executing)[113] and removing the need for trusted intermediaries to manage transactions.[114] Green explains that the aspiration of the smart contract is to replace trust and cooperation in contracting, or the role of the intermediary to produce such outcomes, with the power to code driving execution of the transaction.[115] The reality is no doubt more complex.[116] However, in any event, this is not how most individuals deal with crypto assets.[117] This idea of decentralised, peer-to-peer, trustless transactions has been supplanted by the reality of intermediaries facilitating trade and investment in crypto assets.[118]

One function of intermediaries is to create links between different crypto assets and between crypto assets and fiat-based systems. Put simply, intermediaries are needed to store and exchange access to crypto assets and to move the value of crypto assets in and out of the traditional financial system. Thus, intermediary crypto services include facilitating trades between crypto tokens and fiat money (known as 'on-ramping' and 'off-ramping' from the crypto ecosystem). It also includes issuing and using crypto asset-linked debit and credit cards and creating crypto tokens that represent conventional financial instruments.[119] Examples of intermediary services include centralised exchanges,[120] such as Binance, Coinbase Exchange and (until recently) FTX,[121] which customers buy and sell cryptocurrencies or exchange crypto for fiat currency.[122] Another intermediary service is a digital wallet,[123] which retains the keys needed to transact with digital assets.[124] Still other services include crypto asset

---

Bratanova et al, CSIRO Data61, *Blockchain 2030: A Look at the Future of Blockchain in Australia* (Report, April 2019) 14.

113 Sarah Green, 'Smart Contracts, Interpretation and Rectification' [2018] *Lloyd's Maritime and Commercial Law Quarterly* 234, 236

114 Don Tapscott and Alex Tapscott, *Blockchain Revolution* (Portfolio/Penguin, 2016) 101. See also discussion in Lim, Saw and Sargeant (n 110).

115 Green (n 113) 236. Also Sarah Green and Adam Sanitt, 'The Contents of Commercial Contracts: Smart Contracts' in Paul S Davies and Magda Raczynska (eds), *Contents of Commercial Contracts: Terms Affecting Freedoms* (Hart Publishing, 2020).

116 See also Karen EC Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law' (2017) 3 *Engaging Science, Technology and Society* 1, suggesting that for some, and perhaps many kinds of contractual relationships smart contracts may be wholly inappropriate.

117 *Cryptoassets and Smart Contracts* (n 105) 11.

118 Max Parasol, 'Avoiding the Wholesale De-Banking of Cryptocurrency Exchanges in Australia' (2022) 45(4) *University of New South Wales Law Journal* 1623, 1624; Joseph Longo, 'Crypto-assets: The case for strong regulation and enforcement' (Speech, Australian Financial Review (AFR) Cryptocurrency Summit, 16 October 2023).

119 *Token Mapping* (n 14) 20.

120 See Maurushat and Halpin (n 13) 239; Parasol (n 118) 1632.

121 On FTX see Victoria Bekiempis, 'Sam Bankman-Fried found guilty of defrauding FTX customers out of billions' *The Guardian* (online, 3 November 2023) <https://www.theguardian.com/business/2023/nov/02/sam-bankman-guilty-ftx-alameda>.

122 Kyles (n 99) 140.

123 Maurushat and Halpin (n 13) 240.

124 Kyles (n 99) 139.

custodian services,[125] crypto lending services[126] and schemes for using crypto assets to purchase real-world assets, such as real estate.[127]

B Crypto assets and financial services regulation

The novelty and complexity of crypto assets and the multitude of services associated with these assets raise consumer protection concerns. There have been numerous crypto scams[128] and investor frauds,[129] which have at least partly been enabled by the hype around 'crypto'.[130] Additional risk factors arise from the reality that crypto assets, and the services associated with them, are conceptually complex, legally uncertain, and economically unstable.[131] The Commonwealth Treasury's *Token Mapping Consultation Paper* notes that, while consumers may increasingly see crypto assets as a complement to mainstream investment, many do not understand the ecosystem nor the associated risks.[132] Similarly, Maurushat and Halpin observe that 'consumers are unable to identify which types of cryptocurrencies are legitimate as opposed to those that are fraudulent or so highly speculative as to be predatory'.[133] These concerns have led to calls for tighter financial regulation of crypto assets, and a focus on regulating intermediary services as a way of accessing information about and overseeing otherwise anonymous, untraceable transactions.[134]

In response to concerns about the risks to individual investors from crypto asset products and services, the financial services regulator, the Australian Securities and Investments Commission ('ASIC'), has issued regulatory guidance[135] reminding those who deal in crypto assets of the scope of ASIC's regulatory regime.[136] This guidance

---

125 For a description, see Krisztian Sandor, 'What Is Crypto Custody?' CoinDesk (Blog Post, 12 May 2023) <https://www.coindesk.com/learn/what-is-crypto-custody/>.

126 For a description, see Wayne Duggan, 'Crypto Lending: Earn Money From Your Crypto Holdings' Forbes Advisor (online, 22 September 2023) <https://www.forbes.com/advisor/investing/cryptocurrency/crypto-lending/>.

127 Ilaria Zavoli, 'Cryptocurrencies Transactions in the UK Real Estate Market: Threat or Opportunity for Anti-Money Laundering?' in Doron Goldbarsht and Louis de Koker (eds) *Financial Technology and the Law: Combatting Financial Crime* (Springer, 2022) 67.

128 Eg, Samantha Dunn, 'Facebook Criticised by Australian Tycoon Andrew Forrest Over Deep Fake Crypto Scam', *CCN* (online, 4 February 2024) <https://www.ccn.com/news/facebook-australian-tycoon-andrew-forest-deep-fake-crypto-scam/>.

129 Eg, Luc Cohen and Jody Godoy, 'Sam Bankman-Fried convicted of multi-billion-dollar FTX fraud', *Reuters* (online, 3 November 2023) < https://www.reuters.com/legal/ftx-founder-sam-bankman-fried-thought-rules-did-not-apply-him-prosecutor-says-2023-11-02/>.

130 Pamela Hanrahan, 'How FTX Australia was able to claim it was 'ASIC-licenced', *The Conversation* (online, 13 December 2022) <https://theconversation.com/how-ftx-australia-was-able-to-claim-it-was-asic-licenced-196361>.

131 Longo (n 118).

132 *Token Mapping* (n 14) 5.

133 Maurushat and Halpin (n 13) 259.

134 See World Economic Forum, *Pathways to the Regulation of Crypto Assets: A Global Approach — White Paper* (Report, May 2023) 9. See also Token Mapping (n 14) 5.

135 'Crypto Assets', Information Sheet 225, *ASIC* (Web Page) <https://asic.gov.au/regulatory-resources/digital-transformation/crypto-assets/>.

136 Primarily the *Australian Securities and Investments Commission Act 2009* (Cth) and the *Corporations Act 2001* (Cth).

reiterates that crypto asset intermediaries who are in substance giving financial advice or providing financial services, such through their crypto insurance, wallet, custody, exchanges or investment services, will be subject to licensing requirements and the conduct obligations that accompany licensing.[137] ASIC has further emphasised that it will be vigilant in overseeing crypto asset products and services, including by scrutinising representations that may be misleading[138] and enforcing compliance with the design and distribution obligations.[139]

Despite these efforts by ASIC, the Commonwealth Government has expressed the view that there is ongoing uncertainty about the extent to which the financial services regime applies to crypto assets and related services.[140] In the absence of 'bright line' rules, participants in the market may not be able to precisely ascertain where the line between novel and regulated financial services or products lies.[141] Accordingly, Commonwealth Treasury recently engaged in a 'token mapping' exercise to 'build a shared understanding of crypto assets in the Australian financial services regulatory context'.[142] This exercise has culminated in proposals for more definitive regulatory measures applying to 'platform providers and other intermediaries performing financial services in relation to digital asset facilities (eg brokers, arrangers, agents, market makers, and advisers)' including for greater consumer protection.[143] These entities would be specifically subject to existing Australian financial services laws, including holding a Australian Financial Services Licence and making them subject to minimum standards for holding and transacting in digital assets.[144] Additionally, there are proposals to make a wider number of crypto asset intermediaries subject to KYC laws.

---

137 Ibid. See eg *Australian Securities and Investments Commission v Web3 Ventures Pty Ltd* [2024] FCA 64.

138 ASIC, 'Fintech Company Pays Penalties for Crypto Product Representations' (Media Release 23-261MR, 27 September 2023) <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-261mr-fintech-company-pays-penalties-for-crypto-product-representations/>.

139 ASIC, 'ASIC Sues Crypto Exchange Alleging Design and Distribution Failures' (Media Release 23-256MR, 21 September 2023) <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-256mr-asic-sues-crypto-exchange-alleging-design-and-distribution-failures/>.

140 Senate Select Committee on Australia as a Technology and Financial Centre, Parliament of Australia, *Second Interim Report* (Report, April 2021) 89 [5.56]; John Bassilios and Max Ding, 'Crypto Regulation in Australia: Where are We Now and Where are We Headed?', *Hall and Wilcox* (Web Page, 13 July 2023) <https://hallandwilcox.com.au/thinking/crypto-regulation-in-australia-where-are-we-now-and-where-are-we-headed/>; Longo (n 118).

141 Yadav and Brummer (n 4) 238.

142 Ibid. See also The Board of The International Organization of Securities Commissions, *Policy Recommendations for Crypto and Digital Asset Markets Consultation Report* (Report No CR01/2023, May 2023) (*Digital Asset Markets Consultation Report*).

143 *Regulating Digital Asset Platforms* (n 9).

144 Ibid 12. See also proposals for direct regulation of crypto assets markets in the EU discussed in Tina van der Linden and Tina Shirazi, 'Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?' (2023) 9 *Financial Innovation* 22.

C Crypto assets and KYC

Proposals for extending the application of AML to crypto asset intermediaries arise from concerns about the use of crypto assets for money laundering.[145] Crypto assets represent a way to transfer value other than through traditional financial systems.[146] The relative anonymity, novelty and decentralisation of crypto asset exchanges present opportunities for criminal activities.[147] Crypto assets have been implicated in money laundering[148] and financial crimes.[149] Crypto assets are also the preferred payment system for cyber ransoms and are often used to move scammed payments. The FAFT has repeatedly updated its guidance on countries' obligations to bring crypto or virtual asset service providers under AML law,[150] including mandating the application of KYC laws to crypto asset services identified as posing a high risk of use by criminal networks.[151] The informing principle of these reforms is that crypto asset intermediaries should be subject to the same monitoring obligations as financial institutions,[152] including the requirements of customer due diligence, record keeping, risk assessments and reporting suspicious transactions, already set out above.[153]

Australia already applies the AML regime to cryptocurrency exchange providers operating within its jurisdiction[154] when exchanging digital and fiat currencies.[155] This application means that digital-fiat exchanges are required to register with AUSTRAC as a reporting entity and are subject to KYC verification and reporting requirements, as well as ongoing monitoring.[156] However, the AML designation in Australia currently does not apply where a crypto exchange only involves a trade of one digital currency

---

145 Maurushat and Halpin (n 13) 246–54; Wagman (n 13) 89. On scams, generally see 'Scam Prevention' (n 15).

146 Daniel Dupuis and Kimberly Gleason, 'Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic' (2021) 28(1) *Journal of Financial Crime* 60; Kenneth See, 'The Satoshi Laundromat: A Review on the Money Laundering Open Door of Bitcoin Mixers' (2023) 31(2) *Journal of Financial Crime* 416; European Union Agency for Criminal Justice Cooperation, *Eurojust Report on Money Laundering* (Report, 20 October 2022) 16-17 <https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering>.

147 Doron Goldbarsht and Louis de Koker, 'From Paper Money to Digital Assets: Financial Technology and the Risks of Criminal Abuse' in Doron Goldbarsht and Louis de Koker (eds) *Financial Technology and the Law: Combatting Financial Crime* (Springer, 2022) 6; Wagman (n 13) 88.

148 See (n 146).

149 Goldbarsht and de Koker (n 147) 8; Zavoli (n 127) 69. See also *Digital Asset Markets Consultation Report* (n 142) 54.

150 See 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', *Financial Action Task Force* (Web Page, 28 October 2021) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>; 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Asset Service Providers', *Financial Action Task Force* (Web Page, 27 June 2023) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html> ('Virtual Assets').

151 *Modernising Australia's AML/CTF Regime* (n 6) 13.

152 'Virtual Assets' (n 150).

153 See above n 46-59.

154 Under the *AMLCTF Act* (n 51) s 5, a digital currency exchange ('DCE') provider is defined as a 'registrable digital currency exchange service'.

155 *Modernising Australia's AML/CTF Regime* (n 6) 13.

156 Ibid.

for another digital currency i.e. where no fiat currency is involved.[157] Changes to the regime in Australia have been proposed under the Attorney-General's Department consultation on *Modernising Australia's anti-money laundering and counter-terrorism financing regime*. This Consultation proposes making crypto asset intermediary service providers subject to AML obligations in Australia where they provide any of the following services:

- exchanges between one or more other forms of digital currency;
- transfers of digital currency on behalf of a customer;
- safekeeping or administration of digital currency; and
- provision of financial services related to an issuer's offer and/or sale of a digital currency (eg Initial Coin Offerings where start-up companies sell investors a new digital token or cryptocurrency to raise money for projects).[158]

The Consultation also proposes to amend the so-called 'travel rule'. The travel rule currently requires financial institutions to include payer information for electronic transfers of fiat currency. Payee information is not required. The proposed reforms would require information about the transfer of funds, including for crypto asset exchanges, to include verification of payer information and inclusion of payee information.[159]

Lastly, under the proposal, Australia's AML/CTF regime would apply to a group of purportedly high-risk professions and businesses, including lawyers, accountants, trust and company service providers, real estate agents, and dealers in precious metals and stones.[160] This extension is on the ground that these professions are 'particularly vulnerable to misuse and exploitation by transnational, serious and organised crime groups and terrorists due to the nature of the services that they provide'.[161]

D The impact of extending KYC laws

Several factors must be weighed in assessing the likely impact of the proposed reforms to the scope of KYC in the context of crypto asset providers. Among these considerations are compliance costs, the impact on privacy, and data security. None of these concerns necessarily preclude the KYC laws being extended as proposed; but they indicate the need for care in implementing any reform to a field already beset with tensions between security and privacy, and indeed an overall lack of clarity about the

---

157 Designated services are defined under the *AMLCTF Act* (n 51) s 6.

158 *Modernising Australia's AML/CTF Regime* (n 6) 14. See also Attorney-General's Department, *Paper 4: Further information for digital currency exchange providers (DCEPs), remittance service providers and financial institutions*, Reforming Australia's anti-money laundering and counter-terrorism financing regime (May 2024) <https://consultations.ag.gov.au/crime/reforming-aml-ctf-financing-regime/user_uploads/paper-4-further-information-for-digital-currency-exchange-providers-remittance-service-providers-and-financial-institutions.pdf>.

159 Ibid. See also the discussion of an extended 'travel rule' requiring payer and payee information: Bassilios and Ding (n 140).

160 *Modernising Australia's AML/CTF Regime* (n 6) 17.

161 Ibid.

effectiveness of AML/CTF regimes in combatting criminal activities such as money laundering and terrorist financing.[162]

The costs of complying with KYC laws can be considerable.[163] Podder observes that '[t]here are billions of transactions made each year, so distinguishing and detecting suspicious transactions from the legitimate ones to meet the reporting requirement of AML is a struggle for the banks and the regulators'.[164] Moreover, these laws have been said to contribute to significant, if unquantified, risks of harm through 'de-banking',[165] arising where banks withdraw services to customers due to AML concerns or the costs of KYC, which can impact heavily on individuals,[166] crypto asset businesses,[167] and nation states.[168]

These arguments have a clear application to the proposals to apply KYC laws more widely to crypto asset intermediaries. High compliance costs are likely to be passed onto customers. They may make it more difficult for smaller firms to operate and dissuade new crypto service providers from entering the Australian market. These consequences will have an overall impact on innovation and competition.[169]

It may be accepted that compliance costs are not a conclusive argument against regulation. If the crypto asset activities in question are functional equivalents to the services provided by traditional financial service providers, there is a strong argument for concluding they should be similarly regulated regardless of the novelty of their offering. The goals of investor protection are well accepted and largely effective.[170] In this context it is appropriate to expect crypto asset service intermediaries providing the equivalent financial services to build the capacity to comply with the relevant legislative requirements.[171] By contrast, if the burdens of KYC laws are already excessively

---

[162] Goldbarsht and de Koker (n 147) 7; Suman Podder, 'Leveraging the Provisions of Open Banking to Fight Financial Crimes' in Doron Goldbarsht and Louis de Koker (eds), *Financial Technology and the Law: Combatting Financial Crime* (Springer, 2022) 25.

[163] James Emin, 'Fintech's Financial Crime: Collaboration vs Constraints', *MLROs.com* (Web Page, 2020) <https://mlros.com/fintechs-financial-crime-collaboration-v-constraints/>; 'The Broken State of KYC' (n 86).

[164] Podder (n 162) 25.

[165] Australian Government, 'Government Response: Potential Policy Responses to De-banking in Australia' (Response to Regulatory Advice, June 2023); Senate Select Committee on Australia as a Technology and Financial Centre, Parliament of Australia, *Final Report* (Report, 20 October 2021).

[166] See *Human Appeal International Australia v Beyond Bank Australia Limited* [2023] NSWSC 382.

[167] For example, Charlotte Grieve, '"Denied": NAB, Citi Pulled Banking Services from Fintech Unicorn Airwallex Over Risk Fears', *The Age* (online, 14 April 2021) discussed in Parasol (n 118) 1630. See also discussion of Westpac denying its customers access to Binance a crypto exchange: Josh Taylor, 'Westpac bans transfers to world's largest crypt exchange Binance', *The Guardian* (online, 18 May 2023) <https://www.theguardian.com/business/2023/may/18/westpac-bans-transfers-to-worlds-largest-crypto-exchange-binance>.

[168] See also Doron Goldbarsht, 'Shedding Light on Shadow Banking: The Money or Value Transfer Service Regime in Australia and Its Origins' (2018) 82(3) *Journal of Criminal Law* 264; Emily Lee 'Technology-Driven Solutions to Banks' De-Risking Practices in Hong Kong: FinTech and Blockchain-Based Smart Contracts for Financial Inclusion' (2022) 51(1–2) *Common Law World Review* 83; Parasol (n 118) 1623.

[169] Parasol (n 118) 1643.

[170] Kyles (n 99) 145.

[171] Maurushat and Halpin (n 13) 246–54.

onerous on currently designated reporting entities, with little corresponding impact on crime prevention, more is needed to justify extending the regime further to any new entities, crypto or otherwise.

The proposed KYC law reforms also raise concerns about data privacy protection. If entities seek to collect the information required by the regime without adequate processes for data security, there is a considerable risk to their customers, arising from more significant amounts of personal information being collected and kept longer.[172] The risk may be particularly pronounced in the short-term for firms recently brought into the KYC regime under proposed new reforms. As we have seen, entities complying with KYC are subject to the data protection regime under the *Privacy Act*. However, such firms may lack a sufficiently mature data security model to protect customers' KYC information adequately.[173]

V TECHNOLOGY AS A RESPONSE TO REGULATION AND RISK

A different kind of response to concerns about the impact of extended KYC laws is to try to utilise a technological response to the core concerns, and by doing this reduce the pressure for legal solutions to achieve the key objectives of that regime. Indeed, these technologies may be essential in keeping up with initiatives in money laundering, terrorism financing and proliferation financing.[174]

A Regulatory technology

The growth of novel opportunities for individuals to invest in crypto assets, and the general rise in technological innovation in financial product offerings, are good reasons to consider how technology could contribute to regulatory compliance, oversight and enforcement.[175] The use of technology for regulatory purposes is sometimes described as 'RegTech'. Arner et al explain that RegTech is 'a contraction of the terms "regulatory" and "technology", and describes the use of technology, particularly information technology (IT), in the context of regulatory monitoring, reporting and compliance'.[176] Arner et al further report that within major financial and advisory institutions, 'the majority of RegTech solutions to date have focused on KYC compliance'.[177] At least some KYC tasks, such as collecting and collating information, would seem highly amenable to automation.[178] For example, automating client

---

172 'The Broken State of KYC' (n 86).

173 De Marchi (n 26).

174 Cf Kyles (n 99) 122.

175 Kyles (n 99) 145.

176 Douglas W Arner, Janos Nathan Barberis, and Ross P Buckley, 'FinTech, RegTech and the Reconceptualization of Financial Regulation' (2017) 37 *Northwestern Journal of International Law & Business* 371. See also FATF, 'Opportunities and Challenges of New Technologies for AML/CFT', (France, 2021) ('Opportunities').

177 Ibid 371.

178 Ibid; Doron Goldbarsht, 'Artificial Intelligence and Financial Integrity: The Case of Anti-money Laundering' (2022) 33 *Journal of Banking and Finance Law and Practice* 21; FATF 'Opportunities and Challenges of New Technologies for AML/CTF', Financial Action Task Force (Web Page,

onboarding in a manner compliant with KYC laws may make the process more accurate and cost effective.[179] It has been suggested that developments in machine learning may improve the capacity of firms to flag suspicious transactions[180] and reduce the time spent by humans on the process.[181]

RegTech may equally provide regulators with better oversight of industry compliance with their legal obligations under AML laws and the capacity for timely interventions to trace and recover money trained by crime.[182] RegTech also has a considerable potential to assist in identifying and responding to scams.[183] In Australia, the Commonwealth Government has foreshadowed real-time scam data sharing between financial institutions,[184] ideally through the National Scams Centre.[185] To this end, the Australian Banking Association has recently launched a new fraud reporting exchange platform that 'will enable faster and more targeted communication to help banks stop and recover as much money as possible when customers have paid scammers'.[186] Additionally, the Government has suggested that greater digital collaboration between reporting entities and AUSTRAC is likely to assist in recovering illicit payments.[187]

To date, the possible efficiency gains from using technology in pursuing KYC/AML objectives do not seem to have sparked interest in revising the regulatory regime to reduce the compliance burden on reporting entities or address data protection concerns. Equally, there has to be ongoing scrutiny of the risks associated with increasing reliance on RegTech solutions. Automation, machine learning and

---

July 2021) 5 <https://www.fatf-gafi.org/media/fatf/ documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>.

179 FATF, 'Opportunities' (n 176) [94]; Podder (n 162) 35.

180 FATF, 'Opportunities' (n 176) [4]; Goldbarsht (n 178) 26; Doron Goldbarsht 'Leveraging AI to Mitigate Money Laundering Risks in the Banking System' in Zofia Bednarz and Monika Zalnieriute (eds) *Money, Power, and AI: Automated Banks and Automated States* (Cambridge University Press, 2023).

181 See, eg, 'Building Privacy-Preserving Federated Learning to Help Fight Financial Crime', *IBM* (Web Page, 5 May 2023) <https://research.ibm.com/blog/privacy-preserving-federated-learning-finance>.

182 Doron Goldbarsht, Baskaran Balasingham, and Jeremy Moller 'Open Banking in Australia: Competition and Money Laundering, Risks, and Benefits' (2021) 32(2) *Journal of Banking and Finance Law and Practice* 59, 60–61. See also Hannah Harris, 'Artificial Intelligence and Policing of Financial Crime: A Legal Analysis of the State of the Field' in Doron Goldbarsht and Louis de Koker (eds) *Financial Technology and the Law: Combatting Financial Crime* (Springer, 2022) 281 (discussing RegTech and market manipulation / insider trading).

183 Maurushat and Halpin (n 13) 255.

184 Jim Chalmers, Treasurer and Stephen Jones, Assistant Treasurer, 'Making Crypto Safer for Consumers' (Joint Media Release, Australian Government Treasury, 3 February 2023) <https://ministers.treasury.gov.au/ministers/jim-chalmers-2022/media-releases/making-crypto-safer-consumers>.

185 'How the National Anti-Scam Centre Works', *ACCC* (Web Page) <https://www.accc.gov.au/national-anti-scam-centre/how-the-national-anti-scam-centre-works>.

186 Ibid.

187 'Australian Banks Join New Fraud Reporting Exchange Digital Platform to Help Halt Payments to Scammers', *Australian Banking Association* (Web Page, 16 May 2023) <https://www.ausbanking.org.au/australian-banks-join-new-fraud-reporting-exchange-digital-platform-to-help-halt-payments-to-scammers/>.

artificial intelligence techniques are generally subject to concerns about bias and opacity.[188] This combination of features may amplify concerns about the 'de-banking' of customers without clearly validating those outputs.[189] Regimes such as the EU's General Data Protection Regulation provide rights with respect to data-driven decisions, including the right not to be subject to wholly automated decision-making.[190] Transparency is central to this right and, more generally, accountability for automated decision-making.[191] It is easier for those adversely affected to contest outcomes if they know the basis for the result or even if it was achieved via an algorithm. However, transparency in this context may run against the reason for using digital technologies to provide a covert and rapid response to money laundering or other financial crime activity.

Complementing transparency in ensuring the responsible use of predictive and automated decision-making technologies is the demand for accountability.[192] Accountability mechanisms take many forms but the key objective is to ensure oversight and responsibility for the safe, responsible and effective functioning of AI systems.[193] This principle would require human oversight of any automated system for flagging suspicious transactions. In any event it may be that the element of human judgment is too integral to the process to replace given the high cost of removing or restricting banking services for individuals or businesses.[194]

While a more substantial commitment to data sharing between transacting banks may improve efficiency and reduce compliance costs associated with KYC laws, greater data sharing would also escalate the operation of KYC in encroaching on individual privacy, as discussed earlier. Indeed, a greater reliance on the use of technology to monitor citizens in pursuit of KYC goals of AML might operate to normalise state surveillance of the financial activities of individuals and citizens.[195] Here a possible

---

188 See FATF 'Opportunities' (n 176) [130]-[131].

189 Cf Rebecca L Stanley and Ross P Buckley, 'Protecting the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses' (2016) 17(1) *Melbourne Journal of International Law* 1.

190 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 ('GDPR'), OJ 2016 L119/1, art 22.

191 See eg, 'Australia's Artificial Intelligence Ethics Framework', *Australian Government Department of Industry, Science, and Resources* (Web Page, 7 November 2019) <www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework>.

192 Ibid.

193 OECD.AI 'Accountability' *Policy Observatory* <https://oecd.ai/en/dashboards/ai-principles/P9>. See further Claudio Novelli, Mariarosaria Taddeo and Luciano Floridi, 'Accountability in artificial intelligence: what it is and how it works' (2023) 39 *AI & Society* 1871.

194 Cf Podder (n 162) 25, citing Identitii, 'Simplifying the Data Challenge of AUSTRAC Reporting Entities: The Top Five Challenges Facing the AUSTRAC Reporting Entities' (Web Page, 1 July 2020) <https://identitii.com/austrac-data-challenges/> and noting that even with some process automation, transaction monitoring is highly labour-intensive because human judgment is required to assess potentially suspicious transactions.

195 Daria Impiombato, Yvonne Lau and Luisa Gyhn, 'Surveillance, privacy and agency: Insights from China', *Australian Strategic Policy Institute* (Policy Brief Report No 74/2023) 5, citing Paul Mozur, 'Inside China's dystopian dreams: AI, shame and lots of cameras', *New York Times* (online, 8 July 2018) <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

safeguard may lie in mandating state-of-the-art AI techniques to protect privacy values without compromising data accuracy, for example, federated learning complemented by encryption and differential privacy to allow transaction monitoring without sharing sensitive data held by individual banks.[196] Growing interest in digital identity may also reduce in the volume of personal information held by reporting entities,[197] as discussed further below.

B Digital identity schemes

As has been seen, the key concerns about the KYC laws arise from questions about its efficacy, the amount of personal information held by reporting entities and the compliance costs associated with collecting and safely storing that information. One possible response to these concerns is to systematically integrate the customer verification obligations of KYC within a digital identity regime.[198]

Digital identity schemes are being adopted in many countries,[199] often as a response to the excessive data collection involved in individuals repeatedly having to verify their identities and the associated risks of data breaches.[200] There are a burgeoning number of private providers, including for KYC verification,[201] as well as centralised schemes in which a government body provides the digital identity services.[202] Under a 'federated' model, multiple private identity service providers may authenticate individuals' identities,[203] potentially for both government and private sector services.[204] 'Self-sovereign' models allow individuals to themselves hold the validated identity information, through a chip, sim card or token on a mobile phone.[205]

---

196 'Building Privacy-Preserving Federated Learning to Help Fight Financial Crime' (n 181).

197 FATF, 'Opportunities' (n 176) [92]-[93].

198 *Your Guide to the Digital ID Legislation and Digital ID Rules* (n 8).

199 See, eg, Arthi MC and Kavitha Shanmugam, 'Implementing unique identification technology: The journey and success story of Aadhaar in India' (2023) *Journal of Information Technology Teaching Cases* (India); Bruno Bioni et al, 'The Digitization of the Brazilian National Identity System: A Descriptive and Qualitative Analysis of its Information Architecture' (2022) 4 *Data and Policy* (Brazil); Damian Eke et al, 'Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns' (2022) 11 *Journal of Responsible Technology* 2; Amir Sharif et al, 'The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes' (2022) 12(24) *Applied Sciences* 12679.

200 Explanatory Memorandum, Digital ID Bill 2023 (Cth) [9].

201 See eg, Ekata <https://ekata.com/>; GreenID <https://gbg-greenid.com/advantages/biometrics/>.

202 See eg, Singapore Digital Identity (SingPass) <https://www.smartnation.gov.sg/initiatives/strategic-national-projects/national-digital-identity/#:~:text=Singpass%2C%20the%20National%20Digital%20Identity,the%20current%20suite%20of%20services.>.

203 Axel Domeyer, Mike McCarthy, Simon Pfeier, and Gundbert Scherf, 'How Governments can Deliver on the Promise of Digital ID' *McKinsey & Co* (Web Page, 31 August 2020) <https://www.mckinsey.com/industries/public-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id>.

204 Eke et al (n 199) 2.

205 'Reimagining Digital ID' *World Economic Forum* (Insight Report, June 2023) 6. Cf also 'Putting you in Control of Your Identity', *NSW Government* (Web Page, 1 May 2023) <https://www.nsw.gov.au/nsw-government/projects-and-initiatives/nsw-digital-id>.

Combinations of different verified identity attributes may be available through digital wallets.[206]

The operation of digital identity schemes usually begins with an individual verifying their identity through identity documents, or, in some cases, biometric identification (eg, a faceprint) with an identity service provider.[207] Once this is done, in centralised or federated models, the individual is able to instruct their digital identity provider to confirm their identity to the businesses or government agencies with which they seek to deal. This instruction will be sent via a code, password or biometric identifier (eg, fingerprint, iris scan or faceprint).[208] Relying on a series of cryptographic keys, the digital identity service provider confirms that the identity has been authenticated to the recipient without disclosing the personal information used to verify the person's identity and without itself having visibility on the nature of the transaction contemplated. In self-sovereign models, the individual will themselves hold the key to verifying their identity, usually through a chip, card or wallet.[209]

The overarching characteristic of digital identity schemes is that they allow individuals to choose who to verify their identity with, and in some iterations, what attributes of their identity.[210] In most iterations, a key objective of digital identity schemes is to reduce the amount of personal information shared with businesses and allow individuals to retain control of identifying information.[211] Thus, the Commonwealth Government has promoted its digital identity scheme by explaining that 'Digital IDs provide people with a convenient, re-usable way to verify who they are when transacting online, without having to repeatedly provide copies or details of their most sensitive ID documents'.[212] Ensuring individuals share fewer copies of key identity documents reduces the risks of identity theft that arises from the repeated digital sharing of personal information.[213]

---

206 NSW Government, 'NSW Digital Wallet – a safe and easy way to share your qualifications in NSW'.

207 In practice, the elements of a complete digital identity service may be provided by different entities, see Rajiv Shah, 'The Future of Digital Identity in Australia', *Australian Strategic Policy Institute* (Policy Brief Report No 66/2022, 17 Nov 2022) 6 <https://www.aspi.org.au/report/future-digital-identity-australia>.

208 Shah (n 207) 6.

209 'Reimagining Digital ID' *World Economic Forum* (Insight Report, June 2023) 7.

210 John Fiske, 'Identity Assurance in an Era of Digital Disruption: Planning a Controlled Transition' (Working Paper Series, No 205, Mossavar-Rahmani Center for Business & Government Associate, Harvard Kennedy School, 2023) 4.

211 See Australian Government, 'Why Use a Secure Digital ID?', *Australia's Digital ID System* (Web Page) <https://www.digitalidentity.gov.au/digital-identity-for-you/why-use-a-secure-digital-id>. See also Jo Ann Barefoot, 'Digitizing Financial Regulation: Regtech as a Solution for Regulatory Inefficiency and Ineffectiveness' (Working Paper Series No 150, Mossavar-Rahmani Center for Business & Government Associate, Harvard Kennedy School, 2020), discussing digital identity as a way of distinguishing humans from bots.

212 Explanatory Memorandum, Digital ID Bill 2023 (Cth) [4].

213 See David GW Birch, 'The Best Way to Protect Personal Data? Not to Collect it' *Forbes* (online, 28 November 2022) <https://www.forbes.com/sites/davidbirch/2022/11/28/the-best-way-to-protect-personal-data-not-to-collect-it/>; Australian Government, 'About Digital ID', *Australia's Digital ID System* (Web Page) <https://www.digitalidentity.gov.au/about-digital-identity>.

Again, however, digital identity schemes raise the dilemmas of balancing competing policy objectives and the efficacy of regulating new and emerging technologies. Digital identity reduces the privacy and data protection risks arising from individuals repeatedly sharing identity documents. However, such schemes create new risks centred around surveillance of individuals by identity service providers and governments.[214] For example, many digital identity schemes rely on biometric information for some stage of the process, either verifying the identity of the individual or to authorise sharing of a verified identity.[215] Biometric verification is controversial when used through a centralised database for identifying individuals for a multitude of purposes. The more discrete use of biometric recognition is less controversial, and is already used at passport gates, to unlock devices such as phones. Nonetheless, any use of biometric information in digital identity schemes still raises human rights concerns, including relating bias and inaccuracy.[216] It requires robust regulatory oversight and vigilance against function creep, which would move the technology from providing a secure mechanism for individuals to verify their identity towards a mechanism for tracking the movements of those individuals and the transactions they undertake.[217]

More generally, although digital identity schemes offer enhanced data privacy protection by ensuring individuals share fewer copies of key identity information, they raise concerns about the risk of data breaches centred on the device/location on which information is stored.[218] A centralised government issued identity scheme is reliant on the government building expertise in cryptography and improving data security.[219] A federated scheme involving private providers may prove more innovative but also risks costs associated with those providers withdrawing from the market or lacking the necessary expertise.[220] More generally, the uptake of digital identity schemes depends on customers having confidence in the technology and the providers of the digital

---

214 'Digital Identity and Data Protection: Current Developments and Future Trends', *European Data Protection Supervisor* (Web Page, 22 July 2022) <https://edps.europa.eu/press-publications/press-news/blog/digital-identity-and-data-protection-current-developments-and_en>.

215 For example, the Aadhaar card in India: see Vindu Goel, 'India's Top Court Limits Sweep of Biometric ID Program', *New York Times* (online, 26 September 2018) <https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html>.

216 Mizue Aizeki & Rashida Richardson (eds), Northwestern School of Law Center for Law, Information and Creativity, and Immigrant Defense Project, *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"* (Report, 2021) 16–17.

217 Edward Santow, Sophie Farthing and Lauren Perry, James Martin Institute for Public Policy and Human Technology Institute, 'Improving governance and training for the use of facial verification technology in NSW Digital ID' (Policy Insights Paper, December 2023) <https://jmi.org.au/wp-content/uploads/2023/12/JMI-PIP-Improving-governance-and-training-for-the-use-of-facial-verificationtechnology-in-NSW-Digital-ID.pdf>.

218 'The Future of Identity Verification: Emerging Trends and Technologies', *GreenID* (Web Page, 16 May 2023) <https://gbg-greenid.com/blog/the-future-of-identity-verification-emerging-trends-and-technologies/>.

219 See Erica Mealy, 'A National Digital ID Scheme is Being Proposed. An Expert Weighs the Pros and (Many More) Cons', *The Conversation* (online, 26 September 2023) <https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144>.

220 Shah (n 207) 8.

identity services. At a minimum, this requires providers to be accountable for keeping identity data safe and precluded from using the information for other self-interested purposes. Strong, specific regulatory oversight of both public and private sector providers of digital identity services is only now emerging.[221]

In Australia, the Commonwealth Government committed to supporting digital identity and overseeing digital identity service providers in 2015, beginning with its Trusted Digital Identity Framework.[222] The impetus to move digital identity initiatives forward has been driven by several high-profile data breaches in 2022,[223] which illustrated the harms of excessive data collection and retention by service providers.[224] The Commonwealth operates a digital identity accreditation scheme, myGovID, which includes a digital identity process for access to government services and has proposed extending the uses of this service to private sector transactions requiring age or identity verification.[225] There are also several private providers of digital identity services operating in specific domains.[226]

At the time of writing, the Commonwealth has enacted legislation for a digital identity scheme,[227] which will formalise and expand its existing initiatives.[228] The proposed digital identity scheme in Australia will be voluntary[229] and provide users with a choice of providers.[230] The *Digital ID Act 2024* includes an accreditation scheme for digital identity providers[231] that 'wish to demonstrate compliance with best practice

---

221 Edward Santow, Lauren Perry and Sophie Farthing, 'Digital ID will go mainstream across Australia in 2024. Here's how it can work for everyone' *The Conversation* (online, 11 December 2023) <https://theconversation.com/digital-id-will-go-mainstream-across-australia-in-2024-heres-how-it-can-work-for-everyone-219406>.

222 See 'Digital Economy Strategy 2030' *Website* (Web Page, 2021) <https://www.digitalidentity.gov.au/previousconsultations>.

223 Australian Government, *Australia's Digital ID System: Digital ID Bill – What is it?* (Factsheet, September 2023) <https://www.digitalidentity.gov.au/sites/default/files/2023-09/australias_digital_id_system_legislation_factsheet.pdf> ('*Australia's Digital ID System: Digital ID Bill – What is it?*').

224 Shah (n 207) 3.

225 'Trusted Digital Identity Framework' (n 25). The Hon Bill Shorten, Minister for the National Disability Insurance Scheme, Minister for Government Services, 'Government services in Australia: the next decade' (Speech, National Press Club of Australia, 13 August 2024). See also 'European Digital Identity', *European Commission* (Web Page) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en>.

226 'Trusted Digital Identity Framework' (n 25). See, eg, Digital iD, 'A Fast, Easy and Secure Way to Prove Who You Are', *Australia Post* (Web Page) <https://www.digitalid.com/personal>; 'Seamlessly and Securely Verify Your Customers' Identity in Real-Time', *Mastercard* (Web Page) <https://www.mastercard.com.au/en-au/vision/who-we-are/innovations/digital-id.html>; Your Identity, Your Way', *ConnectID* (Web Page) <https://connectid.com.au/>.

227 *Digital ID Act 2024* (Cth). See also *Australia's Digital ID System: Digital ID Bill – What is it?* (n 223). See also the *Identity Verification Services Act 2023* (Cth) providing privacy protections for identity verification services.

228 Explanatory Memorandum, Digital ID Bill 2023 (Cth) [14].

229 Ibid [11], [320]-[329].

230 Ibid [5].

231 That is, for identity service providers, attribute service providers, and identity exchange providers: Ibid [454].

privacy, security, proofing and authentication standards'.[232] Accreditation will be mandatory for digital identity services providers that seek to participate in the Government's Digital ID system, i.e. providing digital identity to people accessing government services.[233] Providers outside the Government's system may choose to seek accreditation.[234] The accreditation scheme will be supported by 'trust marks', which providers may use to signal their status to the public.[235] Accredited entities must meet requirements for accessibility and useability.[236] The accreditation scheme will further include mandatory privacy protections in addition to what is provided by the *Privacy Act*,[237] including restrictions on the use of biometric identifiers,[238] data profiling[239] and marketing.[240] There will also be obligations on accredited data identity providers to share with the Digital ID regulator notifications of any reportable data breaches.[241] There will be extensive enforcement mechanisms, with penalties for breaches.[242] Responsibility for overseeing and enforcing the digital identity regulatory regime is proposed to be given to the ACCC, with the Office of the Australian Information Commissioner responsible for privacy protections.[243]

The proposed legislative framework is robust and well intentioned. Yet it includes elements for digital identity that raise concerns from consumer and data protection perspectives. The legislation proposes a 'federated' model of digital identity involving multiple commercial providers of digital identity services instead of the government operating the scheme itself. This approach is proposed to enhance 'consumer choice' and 'system efficiency'.[244] This aspiration will only be achieved with safeguards to ensure consumers are able to make informed choices and that providers in the market meet core expectations as to their fitness for purpose, trustworthiness, and security. Trust marks for accredited providers are supposed to support this aspiration. However, the voluntary nature of the accreditation scheme risks exposing consumers to providers with inadequate privacy and security mechanisms outside the government context. There also remain challenges in ensuring that all individuals have access to the technology and are not disadvantaged by not using the scheme.[245]

As noted at the outset, digital identity schemes will impact on the domain of KYC laws. Currently, it is unclear how the two regimes will interact. As the Australian Banking Association points out, there may be digital identity providers that are not

---

232 Explanatory Memorandum, Digital ID Bill 2023 (Cth) [2].
233 Ibid [11].
234 Ibid [11].
235 Ibid [454].
236 Ibid [141]-[143].
237 Ibid [19]-[25], [145]ff.
238 Ibid [23], [72]-[74].
239 Ibid [23], [207]-[211].
240 Ibid [23], [220]-[223].
241 Ibid [160].
242 Ibid [24], [468].
243 Along with a Digital ID regulator, see '2023 Digital ID Bill and Rules submissions', *Australia's Digital ID System* (Web Page) <https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions>.
244 Explanatory Memorandum, Digital ID Bill 2023 (Cth) [4].
245 Fiske (n 210) 4.

subject to KYC requirements and, therefore, on which a KYC reporting entity may not be able to rely.[246] The accreditation requirements for digital identity service providers and KYC requirements may not be the same, which means that consideration will have to be given as to how the regimes are aligned to enhance the policy objectives behind KYC laws and not merely to increase the compliance burden. While the digital identity scheme is still in its infancy and will require ongoing regulatory oversight, privacy in managing personal information is central to the digital identity, as opposed to a secondary consideration. From this perspective, digital identity schemes represent an advance on the treatment of privacy under KYC laws.

C Open banking

In designing a regulatory regime for digital identity that allows coordination between KYC entities, some guidance might be obtained from the Open Banking regime. Open Banking is the first application of the Consumer Data Right ('CDR') in Australia.[247] Essentially, Open Banking applies the framework developed through the CDR to consumer data in a banking/financial services context. This enables consumers to direct a data holder to provide their banking data (such as account and transaction data) in a CDR-compliant format to other participants in the regime, including other banks, financial service providers or companies providing comparison services.[248] The regime is supported by solid consumer protections, including requirements for robust standards of consent,[249] strong privacy standards[250] and an aspiration for a high degree of transparency, such as through dashboards for consumers to continually monitor consent they have given for collecting and using their CDR data.[251]

Much more would need to be done to harmonise the proposed digital identity scheme and KYC requirements with the existing frameworks for Open Banking.[252] However, Open Banking may provide a useful regulatory model because it already contains a robust data handling framework for accredited participants, a framework for data sharing and security, and co-regulation between the ACCC, OAIC and Treasury. Notably, in this context, amendments to the AML regime already allow Open Banking

---

[246] Australian Banking Association, Submission to Digital Transformation Agency, *Digital Identity Submission* (18 December 2020) 2 <https://www.ausbanking.org.au/submission/digital-identity-legislation-consultation-paper/>.

[247] See generally Australian Government, 'What is CDR?', *Consumer Data Right* (Web Page) <https://www.cdr.gov.au/what-is-cdr>.

[248] *Consumer Data Right* (n 30).

[249] Under the Consumer Data Right, consent must be voluntary, express, informed, specific and time-limited: *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) div 4.3 ('*Consumer Data Right Rules*').

[250] *Competition and Consumer Act 2010* (Cth) pt IVD div 5. See also 'Privacy Obligations', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/consumer-data-right/privacy-obligations/>.

[251] See *Consumer Data Right Rules* (n 249) r 1.14. On the scope of the category of Consumer Data Right data, see 'CDR Data', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/consumer-data-right/cdr-data/>.

[252] For example, *AMLCTF Act* (n 51) ss 37A and 38 allow entities to rely on customer identification procedures of third parties in certain circumstances.

participants to rely on other participants' identity verification.[253] Additionally, the emphasis in Open Banking on consumer-centred controls over data and visibility of decisions to share information provides a good aspiration for any more significant move to digital identity as part of KYC laws.[254]

VI CONCLUSION

As an element of AML regimes, KYC laws interact with a host of other initiatives, including (i) innovation in crypto assets, (ii) reform to protect personal privacy, (iii) an enhanced emphasis on data security, (iv) extended financial services regulation, (v) growing capacity for technology to promote regulatory objectives; (vi) digital identity schemes; and (vii) Open Banking. The demands of regulatory coherence direct attention to the points of overlap, duplication and inconsistency between these regulatory regimes. Nonetheless the tension between the regimes cannot be entirely resolved by good design or drafting. The initiatives are informed by different, not always entirely complementary, objectives. There is an undeniable tension between the tendency of KYC laws to compromise privacy in pursuit of oversight of transactions, and the risk of data breaches arising from the collection and storage of personal information. KYC laws may also harm innovation and competition through the costs of compliance. These costs are likely to impact on most heavily on smaller or new entrants to the market and previously unregulated entities.

Crypto assets intermediaries are increasingly subject to regulatory scrutiny under financial services law. It might be entirely acceptable to demand, as the Australian Government has suggested, that crypto asset service intermediaries should be subject to the same KYC obligations as their functional analogues in traditional financial services, and indeed increasingly financial services law applies to crypto asset intermediaries on this basis. Nonetheless, proposed extensions of KYC laws in Australia may justifiably trigger a reappraisal of the regimes monitoring and reporting demands, as compared to the impact of the regime on privacy and data protection. Importantly, if, as numerous scholars have suggested, KYC laws have only limited effectiveness in responding to financial crime then its other impacts are more difficult to justify.

Technology develops quickly and well ahead of considered law reform or measured understanding of its impact. Recognition of the dilemmas of regulating the emerging technology does not mean regulators should be paralysed in the face of the perceived risks of that technology. It demands close attention to these coherence issues

---

[253] Scott Farrell, Australian Treasury, *Open Banking: Customers' Choice, Convenience and Confidence* (Final Report, 2018) 39 (Recommendation 3.4); Doron Goldbarsht, Baskaran Balasingham and Jeremy Moller (2021) 'Open Banking in Australia: Competition and Money Laundering, Risks, and Benefits' (2021) 32(2) *Journal of Banking and Finance Law and Practice* 59, 67. Also Podder (n 162) 19.

[254] How KYC requirements are satisfied within the Open Banking regime will be particularly important should 'action initiation' be introduced as part of the regime, as this shared reliance on verified customer identity information will be essential for facilitating customers switching accounts: *Future Directions* (n 11) 69, 104.

between different regulatory regimes. It may also support taking regulatory initiatives utilising technology seriously as a response to technology-based concerns instead of enacting ever more detailed and potentially rapidly outdated laws. Thus, the tensions between regulatory goals should prompt a closer consideration of using technology to support regulation, which may be deployed as an alternative to existing KYC requirements. Care needs to be taken not to use concern about technological harm as an excuse for automating decision-making that impacts individuals and communities. Nevertheless, properly governed technology may allow more efficient and effective oversight of AML concerns in ways that put less burden on organisations and involve less privacy-harming scrutiny of individuals. There should be recognition of this intermediate ground.

Concerns about the efficacy, cost and privacy consequences of the KYC regime also support investment in privacy-enhancing technology, potentially including digital identity schemes. Again, although these options may reduce compliance costs, they reframe rather than remove the risks to individual privacy and data security. Thus, there should be greater clarity about how the quality and security of digital identity services are best ensured, along with the privacy obligations of digital identity service providers. These issues may seem highly technical. Nonetheless, they act as a reminder of the importance of understanding the entire regulatory landscape in implementing apparently discrete reforms, and that introducing technological solutions may merely move the regulatory dilemmas to another level rather than transcending them altogether.