Reserve Bank of New Zealand
Te Pūtea Matua

10 June 2022

Felix Lee
Via Email: fyi-request-19428-7f164e4f@requests.fyi.org.nz

Dear Felix

Thank you for your request of 23 May 2022 to the Reserve Bank of New Zealand – Te Pūtea Matua made under the Official Information Act 1982 (OIA) for the following information:

- *A copy of all submissions regarding the Future of Money made by the Privacy Commissioner.*

Response

We are releasing a copy of the submission made by the Privacy Commissioner regarding the 'Future of Money - Central Bank Digital Currency' issues paper in full**.** The RBNZ received only one submission from the Privacy Commissioner on topics relating to the Future of Money. A copy of the submission is attached to this letter.

The OIA allows charges to be imposed for the preparation of information in response to requests. The RBNZ is resourced to meet disclosure obligations for a reasonable level of requests and the cost of providing free responses to official information requests is generally borne by taxpayers. However, the RBNZ believes that requesters should bear some of the costs, where allowable under the OIA, when requests are made for large amounts of information, where a response is particularly complex, or where individuals or organisations make frequent requests. In this instance, no charge is being made under the OIA.

You have the right to seek an investigation and review of this response by the Ombudsman, in accordance with section 28(3) of the OIA. The relevant details can be found on the Ombudsman's website at www.ombudsman.parliament.nz.

Please note that we intend to publish a copy of this response on the RBNZ website at www.rbnz.govt.nz/research-and-publications/official-information-requests. Responses to requests are published in order to improve public transparency and provide an additional resource for anyone seeking information.

Yours sincerely

Ross Francis

Ross Francis
Ministerial and OIA Advisor, Government and Industry Relations
Reserve Bank of New Zealand - Te Pūtea Matua

Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Commissioner's submission to the Reserve Bank of New Zealand on *'The Future of Money – Central Bank Digital Currency'* issues paper

Introduction

1. I am pleased to submit on the Reserve Bank of New Zealand (**"Reserve Bank"**) issues paper, *'The Future of Money – Central Bank Digital Currency'* (**"Issues Paper**").

2. This Issues Paper is a discussion on the in-principle case for a central bank digital currency (**"CBDC"**).

3. The Reserve Bank's overall belief is that a CBDC would be a useful development for central bank money because it would both support the value anchor role of central bank money and support the ability of central bank money to act as a fair and equal way to pay and save. The Reserve Bank also rightly identified that a CBDC *"must maintain data privacy"* and that privacy is an important aspect of freedom and autonomy.

Comments

4. The Privacy Act 2020 (**"Privacy Act"**) governs agencies' collection, retention, use and disclosure of individuals' personal information. Under the Privacy Act, one of my functions as the Privacy Commissioner is to examine and comment on proposed policy that may affect individuals' privacy. I hope my comments will assist Reserve Bank officials in thinking about privacy in relation to a future CBDC.

5. Please note that I refer to other CBDC designs throughout this submission. This is meant to encourage officials to consider the privacy enhancing features of these other designs in developing their own CBDC, and not to advocate for any single design.

Identity management

6. The Reserve Bank thinks that a CBDC could support the uptake and use of RealMe or the Digital Identity Trust Framework the Department of Internal Affairs (**"DIA"**) is developing. This implies that a CBDC requires ongoing use of either authentication service. I recommend that the Reserve Bank cautiously considers whether to integrate with existing or future central Government identity verification and management platforms. Furthermore, I am keen to understand whether the Reserve Bank intends that DIA will conduct know-your-customer (**"KYC"**) checks.

Privacy enhancing options may have ancillary benefits

7. Privacy in payments is a feature inherent to the use of cash, but transactional usage of cash is in decline in New Zealand. The introduction of an alternative to private money in the form of a CBDC could well be a positive step toward greater transaction privacy. An interesting staff working paper published by the Bank of Canada tends to confirm this: it suggests that the lack of transaction privacy is leading to problematic price discrimination which would theoretically be remedied through a privacy enhancing electronic cash option.[1]

[1] Garratt and van Oordt, *'Privacy as a Public Good: A Case for Electronic Cash,'* Bank of Canada, July 2019.

8. There are likely more benefits of a CBDC to individuals which could be teased out through further privacy analysis.

Balancing privacy interests with anti-money laundering and countering the financing of terror ("AML CFT") requirements

9. Maintaining privacy and complying with regulation presents a dichotomy: users may want to retain full privacy in transacting, for either legitimate or unlawful reasons. But government agencies usually want to retain some traceability of CBDC balances or tokens to combat money laundering and the financing of terrorism. Society has a strong interest in well-functioning AML CFT regulation which tends to be 'data-hungry' in nature. Clearly, CBDCs should not provide protection for illegal transactions. At the same time, people have a seemingly contradictory yet legitimate interest in maintaining privacy, for example, in relation to their spending habits. A CBDC offers a challenging opportunity to design a form of money that balances these interests.

10. Some design models claim to circumvent Government operated identity management systems whilst also purporting to comply with AML CFT requirements, such as Chaum, Grothoff, and Moser's, published by the Swiss National Bank.[2] Such models leave KYC obligations and AML CFT reporting to commercial banks who can see customer withdrawals for CBDCs and merchant bank deposits. That is, there are CBDC options in which regulators are apprised of critical suspicious transaction information without being privy to transaction histories. I recommend the Reserve Bank seriously consider them.

Privacy is of central importance

11. Obviously not all considerations will be of equal weight when officials come to consider the CBDC design. I think that privacy is essential to a future CBDC and must be prioritised in the design from the outset. Officials need to be wary of placing disproportionate weight on merely desirable design features that may derogate from the features that are crucial to maintaining privacy. For example, the Issues Paper explains that the Reserve Bank is keen to enable offline functionality. However, if this is a bottom-line for the Reserve Bank, it may corner itself into choosing from CBDC models that are not as privacy protective as other models that provide online functionality only.

Token-based or account based

12. The question as to whether the CBDC should be account-based or token-based is really one about the desirability of transaction privacy. We know that transaction information is particularly revealing, and a CBDC that provides a great deal of personal information on citizens is unlikely to attract much buy-in. Put another way, a successful CBDC would need to provide credible transaction protections to gain broad public acceptance. This is certainly true for citizens of European countries. In its *'Eurosystem report on the public consultation on a digital euro'*, the European Central Bank found that privacy is considered the most important feature of a digital euro by both citizens and professionals.

[2] Chaum, Grothoff, Moser, *How to issue a central bank digital currency,* Swiss National Bank, March 2021.

Privacy by Design ("PbD") principles

13. PbD is a well-known approach that calls for privacy to be proactively engineered throughout the design process.[3] The design principles are as follows:

    13.1. *Proactive not reactive* – privacy needs to be part of the planning of any new or updated product, service, system, or process. Privacy considerations should help drive the design rather than being bolted on at the end to address a few privacy risks.

    13.2. *Privacy as the Default Setting* – the default setting of any design should protect the individual's personal information by understanding how the Information Privacy Principles apply in this context.

    13.3. *Privacy Embedded into Design* – privacy should be so integral to the design of the product, service, system, or process that it would not function without the privacy-preserving functionality.

    13.4. Full Functionality – Positive-Sum, not Zero-Sum – design requirements to protect personal information should be treated as an opportunity to design a better product, service, system or process, not as a trade-off with other functionality.

    13.5. End-to-End Security – Full Lifecycle Protection – protection and security of personal information should be considered for every stage of the information lifecycle: collection, storage and security, use, access and correction, disclosure, retention, and disposal.

    13.6. Visibility and Transparency – Keep it Open – how the product, service, system, or process will use the personal information needs to be clear to the individual providing the personal information. The accompanying privacy notice should be written in easy-to-understand, audience-appropriate language.

    13.7. Respect for User Privacy – Keep it User-Centric – at the centre of any design for product, service, system, or process is a person who will use that product, service, system or process. It's that person who will bear the harm and impact of any privacy breach or misuse of their personal information.

14. I recommend the Reserve Bank proactively engineers privacy throughout the design process using the PbD principles.

Consultations with my Office

15. Privacy is not in the sole purview of the Bank and defining it in the context of a CBDC requires consultation with external parties. The Reserve Bank should therefore continue its dialogue with my Office. Public trust in the privacy design the Reserve Bank opts for would be enhanced by Office's input.

[3] digital.govt.nz: https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/

Conclusion

16. To summarise:

    16.1. I would like to better understand what the Reserve Bank intends when discussing the relationship between a future CBDC and RealMe/the Digital Identity Services Trust Framework.

    16.2. I encourage a deeper analysis of the benefits of having a privacy preserving CBDC.

    16.3. The tension between AML CFT requirements and maintaining privacy presents a challenge for the Reserve Bank, but there are interesting models that purport to strike a balance between these interests that officials should investigate.

    16.4. Privacy is an essential feature of a CBDC that should not easily lose out to other features.

    16.5. Transaction privacy is a key factor when considering whether the CBDC should be account-based or taken-based.

    16.6. The Reserve Bank should proactively engineer privacy throughout the design process using the PbD principles.

    16.7. Reserve Bank officials should consult with my Office as it progresses through this work.

17. I trust this submission will be of use to officials as they consider the CBDC's design features. Please contact Ephraim Wilson if you would like to discuss any matters further (ephraim.wilson@privacy.org.nz).

John Edwards
Privacy Commissioner