The Information Commissioner's Office response to the House of Lords Economic Affairs committee inquiry on Central Bank Digital Currencies

Introduction

1. The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the House of Lords Economic Affairs committee inquiry about digital currencies.

2. The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals, providing guidance to individuals and organisations and taking appropriate action where the law is broken. The legislation which the ICO regulates includes: the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003, amongst others.

Response

3. Of the questions posed in the inquiry paper most are outside the ICO's remit. Our evidence is confined to responding to the privacy issues raised in Question 4.

Q4. How should the Bank of England and HM Treasury address concerns over privacy and traceability of payments when exploring CBDC design?

4. We begin by noting that questions over CBDCs cross into many disciplines and regulatory areas, therefore we support a multidisciplinary approach as the right way to take a holistic view and address the numerous challenges posed by CBDCs, including those relating to privacy. We observe also that compliance with UK data protection legislation is required for any organisation transacting with and processing the personal data of UK citizens. Any solution which processes the personal data of individuals, as a CBDC surely will, must comply with data protection law. The ICO believes that data protection should be seen as an enabler of economic activity, because high standards of data protection foster the trust that the public needs in order to realise the potential of data use in financial services, particularly in relation to innovative developments. In the absence of trust and confidence in how personal data is used, the public can quickly disengage from innovative services such as cryptoassets and stablecoins.

5. Common data standards and interoperability will be critical, especially if a CBDC is intended to streamline methods of exchange across currencies. Rigorous attention to high standards of data protection will be necessary alongside these common data standards, to ensure the free flow of data. The ICO has recently responded to government proposals on reform of the UK's data protection legislation, observing that the UK currently has world-leading standards of data protection and that interoperability on a global scale, such as will be required of any CBDC, demands smooth data flows, which in turn requires those high standards of data protection. As a global standard-setter, UK GDPR has the potential to underpin transactions in stablecoins or a Sterling CBDC, setting a global benchmark for other CBDCs to emulate.

6. This will require rigorous adherence to the principles of privacy by design, and data protection by design. Broadly, compliance with data protection legislation needs to be designed-in from the very outset; the nature of CBDC technologies means that the privacy issues will be difficult or impossible to address retrospectively in the latter stages of development, and need to be properly considered as a core element of the design.

7. The correct choice of ledger technology, and careful attention to questions of retention and disposal of transaction data recorded on that ledger, will be central to a solution that properly respects privacy. It may not be possible to separate information on the parties to a transaction from the transaction itself, and where those parties are living individuals it may be appropriate to consider data involved in digital money as a form of personal data. The possibility of greater integration of personal data into financial services means that the principles of data protection are all the more important. The permanent, immutable nature of blockchain technology, for example, is fundamentally at odds with the data retention and disposal principle in UK GDPR, and may prove incompatible with the associated rights to amendment or deletion of personal data.

8. Privacy considerations will require clarity around:

    - The nature of the personal data in question. What personal data will be processed as part of a CBDC transaction and how can this be minimised – how necessary is the sharing of personal data;
    - What are the trade-offs between the right to privacy (anonymity on the ledger) and the public interest in reducing and deterring

financial crime (ie, through access to the ledger data by relevant authorities);

- The purposes for which the data would be used, by all parties to the transaction including intermediary services such as 'wallet' providers;
- How personal data can be secured at all stages of the process, including what happens to it after the transfer has been completed;
- How individuals can exercise their data protection rights, including rights to correction and deletion of data, and associated questions around transparency and accountability in order for their rights to be realistically exercised.

9. The data protection by design process must consider these issues and the underlying data protection principles that they reflect. A full range of options should be examined in order that the risks and benefits of all available solutions are fully considered in the round. At one end of the spectrum of possibilities, a completely closed ledger ecosystem would ensure the sort of privacy and untraceability, even from those running the ledger, enjoyed by citizens when they use cash. At the other end, a ledger which is completely open to all would be utterly transparent so that everybody's transactions were fully visible. This would present a challenge to privacy but might be argued to have social value if it proved effective in deterring financial crime. It is likely that a balance will need to be struck somewhere between these extremes, and where this balance should lie will need very careful examination.

10. In passing, we would note that many current cryptocurrencies appear to be used as speculative and investment vehicles, rather than as reliable methods of exchange, and it is important to maintain a clear distinction between that type of cryptocurrency and the alternatives such as stablecoins and CBDCs.

11. Potentially there may be trade-offs between privacy and wider societal benefits and public interest considerations, such as the use of sophisticated analytical techniques to identify and support vulnerable individuals, or access to the ledger technology to better tackle financial crime, as above. It will be important to establish a firm evidential base for decisions as to where this balance should be struck, and what protections and safeguards will be in place to govern any functions requiring that access. It may also be necessary to consider how the systems may adapt if this balance changes over time. Similarly, if global privacy standards change, systems will need to have the capability to reflect those changes.

12. The CBDC technology is being held up as a possible solution to settlement friction in existing global financial systems, for example in the Bank for International Settlement (BIS) work on enhancing cross-border payments[1]. It is important that any benefits which may be realised here are not allowed to override considerations of privacy if the public is to accept and trust this technology and, again, a proportionate balance will need to be determined between privacy and any international considerations.

13. The CBDC concept envisages that there will be providers of digital 'wallet' services and other intermediaries who provide access to the CBDC at a consumer level. These are likely to seek to monetise their user data to fund their services. This will raise important questions in relation to the fairness and purpose-limitation principles which remain at the heart of the UK GDPR. If this monetisation constitutes unfair or incompatible exploitation of users' data, it will be important to ensure that effective regulatory safeguards remain in place. This will require that effective provisions extend beyond the borders of the UK and that wallet providers and similar services can be properly regulated, including by the ICO and FCA, wherever they interact with UK individuals.

14. Similarly, banks and other financial institutions are obliged to undertake 'know your customer' due diligence checks on their account holders, to prevent money laundering and terrorist financing offences. Wallet providers are assumed to need to undertake similar due diligence, and all these checks raise important issues of privacy and data protection which will need to be carefully considered.

15. Access to the ledger via third party wallet providers will create potential vulnerabilities and any design will need the highest levels of security to ensure that any such nodes of access cannot be exploited to compromise the ledger. Similarly, reliability of service will be vital, especially if a CBDC is envisaged to be the main or even sole mechanism of exchange. The ICO's work for our role under the Network and Information Systems Regulations 2018 in regulating online marketplaces, search engines and cloud services, shows that critical infrastructure has the potential to have catastrophic effects on businesses and individuals if it fails.

16. The ICO has already indicated to HM Treasury and the Bank of England that it stands ready to assist the CBDC Taskforce and expects

[1] Enhancing cross-border payments: building blocks of a global roadmap (bis.org)

to remain closely involved in the work as it progresses. We therefore wish to assure the committee of our readiness to provide expertise to assist with these difficult questions of balance between privacy and the public good.

Stephen Bonner

Executive Director (Regulatory Futures and Innovation) 15 October 2021