Central Bank Digital Currency Data Use and Privacy Protection

Kieran Murphy, Sun Tao, Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, and Kristina Miggiani

NOTE/2024/004

FINTECH NOTE

Central Bank Digital Currency Data Use and Privacy Protection

Prepared by Kieran Murphy, Sun Tao, Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, and Kristina Miggiani[1]

August 2024

[1] With contributions from Padma Sandhya Hurree Gobin and Jose Carlos Moreno Ramirez (STA), Maria Soledad Martinez Peria and Itai Agur (RES).

Central Bank Digital Currency Data Use and Privacy Protection

Note 2024/004

Kieran Murphy, Sun Tao, Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, Kristina Miggiani*

Cataloging-in-Publication Data
IMF Library

Names: Murphy, Kieran Patrick, author. | Sun, Tao, 1970- , author. | Zhou, Yong Sarah, author. | Tsuda, Natsuki, author. | Zhang, Nicolas, author. | Budau, Victor, author. | Solomon, Frankosiligi, author. | Kao, Kathleen, author. | Vucinic, Morana, author. | Miggiani, Kristina, author. | International Monetary Fund, publisher.
Title: Central bank digital currency data use and privacy protection / Kieran Murphy, Sun Tao, Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, and Kristina Miggiani
Other titles: CBDC data use and privacy protection. | Fintech notes.
Description: Washington, DC : International Monetary Fund, 2024. | NOTE/2024/004. | Aug. 2024. | Includes bibliographical references.
Identifiers: ISBN:
9798400286971 (paper)
9798400287176 (ePub)
9798400287275 (WebPDF)
Subjects: LCSH: Finance—Technological innovations. | Data privacy.
Classification: LCC HG173.M8 2024

RECOMMENDED CITATION: Murphy, Kieran, Sun Tao**,** Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, and Kristina Miggiani. 2024. “Central Bank Digital Currency Data Use and Privacy Protection.” IMF Fintech Note 2024/004, International Monetary Fund, Washington, DC.

Publication orders may be placed online, by fax, or through the mail:

International Monetary Fund, Publications Services
P.O. Box 92780, Washington, DC 20090, USA
Tel.: (202) 623-7430 Fax: (202) 623-7201
E-mail: publications@imf.org
bookstore.IMF.org
elibrary.IMF.org

*This note was written under the supervision of Dong He. It has benefited from comments by several IMF staff members. The authors would especially like to thank Tommaso Mancini-Griffoli for valuable comments.

Contents

Acronyms

AI ..... Artificial Intelligence

AML ..... Anti–Money Laundering

CBDC ..... Central Bank Digital Currency

CCPA ..... California Consumer Privacy Act

CFM..... Capital Flow Measures

CFT ..... Combating the Financing of Terrorism

DNS..... Deferred Net Settlement

ECB ..... European Central Bank

FPS ..... Fast Payment Systems

GDPR ..... European Union's General Data Protection Regulation

KYC ..... Know Your Customer

MPC ..... Multiparty Computation

PET ..... Privacy Enhancing Technology

PII ..... Personal Identifiable Information

PSP ..... Payment Service Provider

ZKP ..... Zero Knowledge Proof

1. Introduction

Central bank digital currency (CBDC), as a digital form of central bank money, may allow for a "digital trail"—data—to be collected and stored. In contrast to cash, CBDC could be designed to potentially include a wealth of personal data, encapsulating transaction histories, user demographics, and behavioral patterns. Personal data could establish a link between counterparty identities and transactions.

Like other payments data, CBDC data may have economic value. Data are non-rival. Data are infrastructural resources that can be used by an unlimited number of users and for an unlimited number of purposes as an input to produce goods and services (OECD 2015). CBDC data could potentially be harvested by financial institutions that, in turn, could help develop data-driven businesses.

Furthermore, CBDC data use could help central banks achieve policy objectives. It could help reduce information asymmetries, potentially assist in supporting financial inclusion, facilitate payment system interoperability, and promote innovation and market contestability. It could provide more timely information about the state of the world and help improve macroeconomic policymaking and regulatory compliance. Data use by central banks differ from that of law enforcement and national security authorities, which may be vested with powers under national legal frameworks to lawfully access personal data. If permitted by the relevant laws, CBDC data use could allow for increased traceability for such authorities to track or prevent illicit and fraudulent activities.

Many central banks already have access to personal data and have experience in data protection that could be applied to CBDC data use. Central banks operate payment systems today such as fast payment systems (FPS). All personal data processed by such systems have to be in accordance with local data protection laws and standards. As a result, many central banks have an understanding of requirements for protecting personal data before launching a CBDC.[2]

CBDC data use, however, could pose risks to privacy, which, in turn, can undermine the trust in central bank money. Privacy can include the protection of someone's personal space and the right to be left alone; the control over and safeguarding of one's personal information; and an aspect of dignity, autonomy, and ultimately human freedom (Acquisti, Taylor, and Wagman 2016). Some authors have argued that privacy is inherent to the nature of money (Kahn, McAndrews, and Roberds 2005). If poorly designed or managed, CBDC personal data use could pose risks to privacy, arising from events such as data leakages, data abuses, cyberattacks, and cross-border payments data flows, thus also negatively affecting CBDC adoption. Indeed, technology alone cannot ensure privacy protection. For instance, even anonymized[3] transactions can be reidentified and the data can be de-anonymized with metadata (Fleder and Shah 2020).

[2] See as examples: Privacy statement for T2 (europa.eu) and Federal Reserve Board—Privacy Program.

[3] Privacy is not synonymous with anonymity (Auer and others 2021). Transactions are anonymous when the identity of the transacting parties is not revealed or is unknowable. Transactions are private if transaction-relevant data (for example, the amount and the timing of the transaction) are not revealed.

Privacy concerns are increasing over time (Goldfarb and Tucker 2012a). However, the notion of privacy is not consistent across the globe and laws vary significantly by region.[4] Privacy is a complex issue and difficult to define—privacy means different things to different people whose own preferences may also be ambiguous. Consumers are often in a position of imperfect or asymmetric information regarding when their data are collected, for what purposes, and with what consequences. Discrepancy between attitudes and behaviors—the "privacy paradox"[5]—shows that individuals may claim more privacy concerns than their behavior indicates. The privacy paradox makes it difficult to calibrate the appropriate policy interventions.

While many privacy concerns are already apparent in existing digital payment systems, CBDCs could present new challenges. CBDCs could be perceived as an instrument for state surveillance. Some may worry that the government or the central bank could use it to control or restrict payments users can make with CBDC, thereby undermining public trust in central bank money. These worries persist despite the private sector often having extensive access to data, which is generally widely accepted and uncontested in comparison to concerns raised about official sector data gathering and usage. It can be a particular concern in countries with severe governance and corruption vulnerabilities. However, public attitudes toward state surveillance versus commercial surveillance also differ across countries.

Whereas some societies trust commercial entities more than government institutions, it could be the other way around in other societies. In its 2024 annual survey of 32000 people in 28 countries, Harvard Business School's Institute for the Study of Business in Global Society and the Edelman Trust Institute found that, when averaged over all 28 countries, more respondents trust business (63 percent) than trust government (51 percent).[6] However, when the results are examined at individual country level, government is trusted more in 4 countries and business is trusted more in 24 countries.

Central banks face important trade-offs when designing CBDCs: they need to strike a balance between CBDC data use and privacy protection. Similar to other digital payments, such trade-offs for CBDC may differ from country to country, depending on cultural norms, societal preferences, legal requirements and traditions, and the degree of public trust in public institutions versus private ones. In addition, the degree of trade-off could depend on the degree of the granularity of data: where aggregate grouped data is sufficient to extract value, the trade-off could be inexistent—to the extent that users can be convinced that their individual data will not be used. Where granular personal data is needed to extract value, the trade-off could be much higher.[7]

This note offers a framework to help countries navigate, as well as tools to help them manage, the trade-off between CBDC data use and privacy protection. This chapter addresses retail CBDC, as data access

[4] World Economic Forum, Privacy and Confidentiality Options for Central Bank Digital Currency, November 2021, https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.

[5] The term "privacy paradox" was first coined and documented by Athey, Catalini, and Tucker (2017), although empirical studies focusing on digital payments since have found a significant role of privacy suggesting no paradox for digital payments specifically (for example, European Central Bank 2022).

[6] See https://www.edelman.com/trust/2024/trust-barometer.

[7] It should be noted that some consensus has already been achieved on elements of this trade-off within the international community, such as on the application of anti–money laundering (AML) and combating the financing of terrorism (CFT) laws and regulations to CBDC.

and privacy-preserving considerations in a wholesale environment are similar to those of the traditional RTGS systems. It emphasizes the role of institutional arrangements, data collection, access and storage policies, design choices, and technological solutions. At a given level of preference for privacy, central banks can facilitate better use of CBDC data through robust transparency and accountability arrangements, sound policies, and judicious adoption of privacy-by-design approaches including the use of privacy-enhancing technologies (PETs).

Summary of Findings

CBDC offers an opportunity to possibly improve the trade-off between data use and privacy protection as compared to private digital payment systems. Facing a similar trade-off to private digital payment systems, central banks may have several potential advantages in striking a better balance. They have strong convening powers and are well positioned to clearly articulate principles and policies to enable privacy and coordinate the adoption of a privacy-by-design approach in the CBDC ecosystem. Central banks could strengthen communication and consumer education to reduce privacy concerns. They could offer a diverse set of CBDC design choices to cater to different preferences for privacy. Central banks could promote innovation and competition by avoiding data silos and encourage data sharing. Finally, central banks are also in a better position to coordinate with other competent agencies to ensure consistency in legal and regulatory frameworks to build trust in CBDCs.[8]

Given the potential diversity of preferences for privacy, central banks may wish to offer a variety of CBDC designs to cater to the privacy needs of different users. For small value transactions, CBDCs could be designed as close substitutes for cash, providing a high degree of privacy to users. In this case, robust institutional arrangements, policies, and technological solutions should be adopted to ensure that CBDC use is compliant with anti–money laundering/combating the financing of terrorism (AML/CFT) laws and regulations, at a level at least as good as cash. Note that cash is largely anonymous — meaning it can be used for illicit transactions. A variant of this design choice for small value transactions could allow better identification of personal information of the user, if the user so requests. For instance, such users may be interested in allowing their payment data to be used for credit scoring purposes if they have a higher chance of obtaining credit.

Central banks may be in a better position to avoid data silos and promote market contestability by facilitating efficient and safe CBDC data sharing among market participants. For larger value transactions, CBDC data use could afford a similar level of privacy protection as other digital payments. In those cases, the payment service providers (PSPs) would collect and store CBDC data just as they collect and store data from other digital payment services. Even if the central bank does not have access to or store those CBDC data, it can set up mechanisms to encourage CBDC data sharing among PSPs while protecting privacy. Such sharing of CBDC data could help promote market contestability and improve the efficiency of financial services.

[8] While the central bank will undoubtedly play a role, the decision as to whether and how to use CBDC data and protect privacy may need to be made jointly by the central bank, the government, and other relevant policymaking bodies, depending on legal and institutional requirements in different jurisdictions.

Technology can help protect privacy through the adoption of privacy-by-design approach but needs to be complemented by rigorous regulatory requirements and institutional safeguards. Technology offers flexibility in design to share data legitimately by accommodating diverse preferences and situations. Technology can allow a range of privacy options. It can help convince users what data can be accessed for law enforcement, for instance, through “proofs of correct execution.” These “proofs” can be audited and communicated to users to build trust. Nevertheless, technology alone will not be sufficient to ensure trust. Rigorous legal and regulatory requirements and sound institutional safeguards on transparency and accountability will be necessary to convince users that technology will not be misused, and perpetrators of privacy infringement will be prosecuted.

More generally, rather than a uniform solution to protect privacy, a nuanced approach—dynamic and individualized to specific markets, legal systems, contexts, and scenarios—may be necessary. Policymakers must communicate with the public to provide information on the implications of different CBDC design choices for privacy. They must also set up institutional mechanisms to ensure that established principles, policies, and laws for privacy protection are implemented; stakeholders are compliant; and violators are held accountable.

However, simultaneously with individualized solutions, a coordinated approach should be considered for cross-border data flows associated with CBDC data use and privacy protection. CBDC cross-border data flows face similar privacy risks as other private digital cross-border payments. While it is understandable that data use and privacy standards differ across countries, stringent data localization regulations will be an impediment for cross-border use of CBDC. The international community is working on addressing these issues, striving for harmonization of standards to promote free cross-border data flow while ensuring privacy, oversight, and protection.

2. CBDC Data Generation

This section discusses how CBDC design and operating models would determine the type of data that can be generated, stored, and used. It first describes how and what data are typically generated in different types of digital payments and then compares and contrasts them with CBDC data generation.

Payment data can be clustered into the following categories:

- **Payer's/payee's identity** refers to identifiers and attributes[9] certified to being associated with a counterparty.[10] Identification of parties to a transaction, typically provisioned through verifiable credentials (like official papers or digital documents), is required for regulatory purposes (including AML/CFT).[11]
- **Payer's/payee's pseudonymous identifiers** make it possible for a counterparty to participate in a payment transaction, without necessarily revealing its identity. These identifiers are usually part of the money representation (account number or token address that belongs to, or is controlled by, a counterparty), but can also be proxied by optional representations of the counterparties themselves (such as phone numbers or aliases).
- **Transaction data** represents the minimum data elements required to make up a payment transaction. It usually consists of the transferred amount and, for practical reasons, the date of the transaction (or timestamps generated during its lifespan).
- **Payer additional transaction data** designates the optional metadata that can be generated on the payer's side beyond what is necessary for a transaction. It is only proposed by some payment instruments (like credit transfer) and can include payment reference or other free-form text payload transmitted to the payee (such as an invoice number for easier reconciliation).
- **Payee additional transaction data** groups several metadata elements generated on the payee's side during the payment transaction that describes the context of a purchase beyond what is necessary for a transaction. They include itemized data points such as merchant's name, purchase location, and spending category. Subject to contractual agreements between PSPs and merchants, this category can considerably evolve to enable new use cases and reap the economic benefits of rich merchant-side data.

Examples of data generation in existing digital payments include the following (Table 1):

- **Credit transfer** between bank accounts can generate payer's transaction data to convey an optional message to the payee. This could include identifying information required for compliance with regulatory requirements, such as capital flow management measures (CFMs) in cross-border payments and AML/CFT rules.

[9] Personal data in addition to identifiers such as gender, race, and income level.

[10] The certification, and often the issuance, of these identifiers is usually done by the government and public agencies or their delegates.

[11] Identification of a customer is an important part of the customer due diligence process, which—along with other preventive measures—is a requirement under AML/CFT rules where certain circumstances exist (for example, when a customer relationship is established or in the case of occasional transactions above a stipulated threshold).

- **Card payments** can generate transaction data on the payee's side, such as the name and location of a merchant and spending category for the purchased items, which can be used for fraud monitoring, credit assessment, and marketing intelligence.
- **E-money** can generate data on the payer's and payee's transactions, although the arrangements differ across PSPs, depending on their instrument designs.[12]

Table 1. Data Generated by Various Payment Instruments

Data Generation (by type of instrument)	**Cash**	**Credit Transfer**	**Card**	**E-Money Instruments**
Payer's IDENTITY - name, DOB, address, digital ID				
Payer's pseudonymous IDENTIFIERS - account number / token address(es) / phone number / alias				
Payee's IDENTITY - name, DOB, address, digital ID				
Payee's pseudonymous IDENTIFIERS - account number / token address(es) / phone number / alias				
Transaction DATA (minimum) - amount, date				
Payer additional transaction DATA - payment reference, invoice number, payment purpose, and so on				
Payee additional transaction DATA - merchant name, location, spending category, and so on				
Source: Authors	*Legend:*	Instrument dependent	Yes	No

CBDC Data Generation

CBDC data generation depends on the retail CBDC's operational model. CBDC payment transactions can potentially offer a wealth of personal data encapsulating transaction histories, user demographics, and behavioral patterns. Two CBDC operational models are being explored: one-tier and two-tier.

[12] The EU's E-Money Directive for example defines e-money as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer." See definition and data collected in https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html.

- **In a one-tier model,** central banks would perform all the necessary functions, including client-facing and resource-intensive tasks that may not fall into their traditional mandate. This implies that the central bank could be the main collector and repository of identity and transaction data. The one-tier model may be considered theoretical, as most central banks exploring CBDC are not considering this option.
- **In a two-tier model,** however, PSPs also collect and store CBDC data, with varying allocation of roles.[13] As most central banks exploring CBDC are considering a two-tier operational model given that it preserves the role of PSPs, including intermediaries, this note focuses on the two-tier models of retail CBDC.

Some designs generate very little or no personal data. For large value transactions, central banks generally require more information on identity, including for AML/CFT purposes (high data intensity). For small value transactions, some central banks, such as China and Nigeria, are pursuing more privacy-enhancing features in their designs, which require less information on identity and transactions (low data intensity). For example, both China and Nigeria apply tiered customer due diligence (CDD). In both models, no or minimal personal identifiable information is required to be collected in the lowest CDD tier.[14] Using a "managed anonymity" approach, the lowest "Know Your Customer" (KYC) tier in China only requires a phone number to open an account (although ID is needed to get a phone number), which prevents the central bank and PSPs from accessing the personal identifiable information (PII).[15]

The data intensity of CBDC design and operating models determine who and what data can be accessed, stored, and used (Table 2):

- In a high data intensity design, identity and transaction data of both transacting parties are recorded, and PSPs of both the payer and the payee are likely to have access to such data.[16] Access by the central bank to the identity and transaction data of both the payer and payee, however, is dependent on design.
- In a low data intensity design, transactions could be made by using pseudonymous identifiers with identity data only known by the parties generating such data. In addition, transaction data may be known only between the payer and payee and the ledger administrator while additional transaction data, as described at the beginning of this section, may not be shared with others. Therefore, the central bank may not have access to identity and transaction data.

[13] Within the two-tier model, privacy protection could be different between the intermediated model and the hybrid model. In an intermediated model, the central bank does not record retail transactions, but only records the account balances of PSPs. All the detailed records of retail transactions are maintained by the PSPs. By reducing the concentration of data, such designs could also enhance privacy. In a hybrid model, the PSPs perform all consumer-facing payment services but the central bank regularly receives a backup of transactions and account balances of individual users (Auer and Boehme 2021). Such designs could enhance privacy, but to a lower degree than that of an intermediated model.

[14] It should be noted that the standard setter has not weighed in on such threshold approaches and no countries have had their CBDC arrangements assessed for compliance with the international standard. Financial integrity implications of different CBDC models will be covered in a separate Fintech Note.

[15] People's Bank of China 2021.

[16] Pursuant to FATF recommendation 16 (that is, wire transfer rule), information on both the payer and payee (for example, name, address, account number) would need to accompany the wire transfer and remain with the transfer throughout the entire payment chain.

Table 2. High and Low Data Intensity Designs of CBDC

Data Access for High-Intensity CBDC	Payer	Payee	Payer Intermediaries	Payee Intermediaries	Operator (Central Bank)
Payer's IDENTITY					
Payer's pseudonymous IDENTIFIERS					
Payee's IDENTITY					
Payee's pseudonymous IDENTIFIERS					
Transaction DATA					
Payer additional transaction DATA		Some elements		Some elements	
Payee additional transaction DATA					
Data Access for Low-Intensity CBDC	Payer	Payee	Payer Intermediaries	Payee Intermediaries	Operator (Central Bank)
Payer's IDENTITY					
Payer's pseudonymous IDENTIFIERS					
Payee's IDENTITY					
Payee's pseudonymous IDENTIFIERS					
Transaction DATA					
Payer additional transaction DATA					
Payee additional transaction DATA					

Source: Authors.

Legend: Likely | Unlikely | Design dependent

Commonalities exist between CBDCs with high data intensity designs and traditional retail payment systems. While traditional retail payment systems, such as deferred net settlement (DNS) systems, are generally private sector operated and therefore not directly comparable to CBDC, some FPS are operated by central banks. This has allowed central banks to build experience in collecting, storing, and using personal data. In those schemes, data access and use have to adhere to privacy protection and

consumer protection laws, protecting privacy while at the same time allowing conditional access to FPS data for regulatory purposes (see more discussion in section 5 “Tools for Managing the Trade-off between CBDC Data Use and Privacy Protection”).

Other stakeholders could be granted access to data, based on their mandates. For example, law enforcement authorities and financial Intelligence units may have access to the aforementioned data pursuant to the execution of their mandates. Conditions for such access should be stipulated in a fair, lawful, and transparent manner, for example, through legislation or regulation, or pursuant to court orders. Statistical authorities may have access to aggregated data with a level of granularity that would depend on the data-sharing practices in the jurisdiction.

3. CBDC Data Use and Risks to Privacy Protection

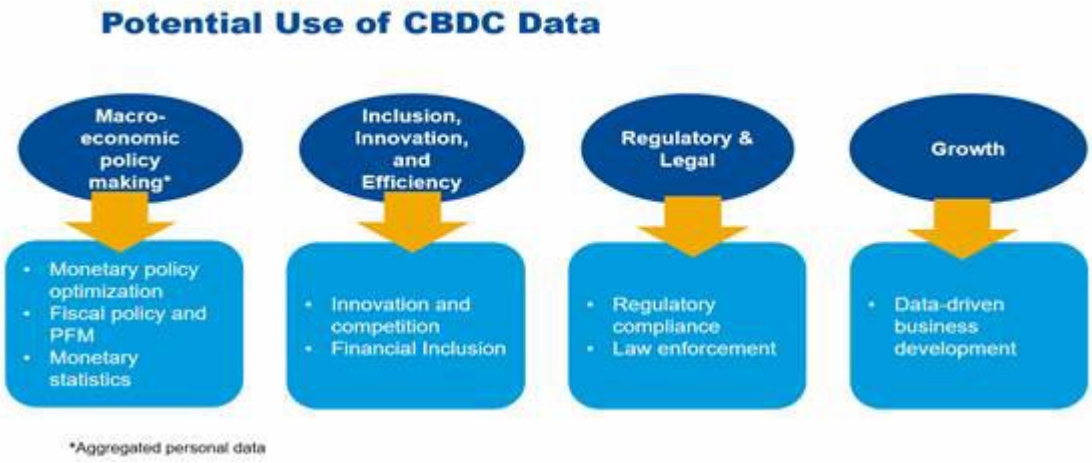
The previous section discussed the type of data that could *potentially* be generated depending on different CBDC designs and operating models.

However, whether and how such CBDC data will be used is a matter of choice by the central banks concerned. Some central banks have adopted a policy position where they will not be able to access or use CBDC personal data. For example, this is the case for the European Central Bank (ECB)[17] and the Bank of England.[18] In contrast, other central banks (for example, the Reserve Bank of India[19]) have emphasized the economic value of CBDC data.

This section assumes that the central bank is interested in exploring the use of CBDC data while ensuring privacy. It discusses how data generated by CBDC usage, either aggregated group data or individual personal data (for example, identity and transaction data), can be used to achieve certain policy objectives and how their economic value can be realized (Figure 1). It then discusses how CBDC data use could pose risks to privacy protection.

CBDC Data Use

Figure 1. CBDC Data Use



Source: Authors.

[17] The Eurosystem will not be able to identify people based on their payments. Personal transaction details from offline digital euro payments would be known only to the payer and the payee. See https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html.

[18] Legislation would be introduced for any digital pound to guarantee users' privacy and control. See https://www.gov.uk/government/news/bank-of-england-and-hm-treasury-respond-to-digital-pound-consultation.

[19] Reserve Bank of India, "Concept Note on Central Bank Digital Currency," page 20, October 2022.

Macroeconomic Policymaking

- **Monetary statistics**. CBDC data, particularly aggregated transaction and position data, could help refine monetary statistics. These data could facilitate a more accurate representation of monetary aggregates and serve as real-time economic indicators. For example, having geographical aggregate views could improve the monitoring of real-time shock propagation,[20] and having sectoral aggregate views could help monitor the effectiveness of real-time monetary interventions (Annex I and II).
- **Monetary policy optimization.** Central banks could leverage aggregated CBDC transaction data to gain real-time insights into consumption and investment, informing monetary policy decisions to achieve macroeconomic objectives like inflation, unemployment, and economic growth.
- **Fiscal policymaking.** Fiscal authorities (including ministries of finance) could leverage CBDC data involving government payments—that is, data from transactions that use CBDC for revenue collection and payments—to enhance data accuracy and timeliness of financial reporting, strengthen data quality to inform fiscal policymaking, facilitate targeted fiscal transfers and streamline service delivery to citizens, and enable better traceability/audit trail of government-related financial transactions for accountability.[21]

Inclusion, Innovation, and Efficiency

- **Innovation and competition.** CBDC PSPs can use CBDC data to identify underserved market segments and develop customized financial products such as microloans or savings plans that cater specifically to the consumers' needs. Granting PSPs access to CBDC data could lower the barrier to entry and reduce the dominance of large financial institutions.
- **Financial inclusion.** CBDC data could provide a comprehensive payment and financial history for individuals and small businesses, who may lack traditional credit histories. Those data could be analyzed to identify the financial needs of various user segments, particularly those that are underserved and without credit records[22] (Annex III).

Regulatory Compliance and Law Enforcement

- **Regulatory compliance.** CBDC data could help strengthen the implementation of a country's regulatory framework, including AML/CFT rules. PSPs in a CBDC ecosystem should use the data to identify customers or parties to transactions, verify such identity, and collect data to understand and monitor customer relationships. CBDC systems could also automate CFMs through smart contracts leveraging real-time CBDC data. These have been referred to as "smart CFMs" (He and others 2023).

[20] See Orestes (2023) study using the Brazilian instant payment system PIX data to track a frost shock across agricultures and cities in Brazil. Mentioned in Banco do Brasil's LIFT Papers v5 n5, "Brazil's Central Bank Digital Currency: Improving Financial Infrastructure with Programmability."

[21] To facilitate fiscal transfer and enable traceability, government may allow intermediaries, to access and use personal data following privacy protection principles and polices in their jurisdictions.

[22] See more discussion on financial inclusion in Lannquist and Tan (2023), and Committee on Payments and Market Infrastructures (CPMI) and World Bank (2020).

- **Law enforcement.** Where governed by a robust legal and institutional framework, CBDC data could increase traceability and transparency of transactions, which could deter illicit activity, and further criminal justice efforts. Access to identity, geolocation, or transaction data can bolster the capacity of law enforcement agencies in tracing the flow of funds related to illicit activities. Even without identity data, Artificial Intelligence (AI) and other tools can improve understanding of trends, patterns, and flows, and help flag anomalies.[23]

Growth

- **Data-driven business development.** CBDC identity and transaction data offer new avenues for monetization, particularly for PSPs. Data use could have current and potential benefits, such as financial planning and credit scoring (Annex III). By analyzing spending patterns and consumer preferences, CBDC PSPs and merchants can create value-added services that meet the evolving needs of consumers and thus develop data-driven business models.[24]

Risks to Privacy

While CBDC data use can bring benefits to societies, it could raise privacy concerns, as poor designs and lack of institutional safeguards could cause users to lose control over who has access to their personal data and how such data would be used. Privacy is a human right[25] and fundamentally pertains to the boundaries between the self and the others, between private and shared, or, in fact, public (Acquisti, Taylor, and Wagman 2016). Because of externalities, where benefits of using CBDC data do not necessarily accrue to the individual users, there may not be sufficient incentives in the CBDC ecosystem to protect the privacy of individual users. Conversely, an individual may not want their personal data to be accessed or used by others if they do not benefit from such data use.

In this context, if poorly designed or managed, CBDC data use could pose the following risks to privacy:

- **Data leakage.** Data leakage refers to unauthorized or accidental exposure of personal data including sensitive information. In the context of CBDCs, this could involve transaction-generated personal data or identity information becoming accessible due to security flaws or mishandling. Such leakage can lead to identity theft, financial fraud, and a loss of public trust in the CBDC system.

- **Data abuse.** Even when personal data are obtained legally, there is a risk of abuse. This includes unauthorized use of personal data by third parties or even by the CBDC issuing authority and governments, for purposes other than those for which it was originally collected and consented to by the users. This is a significant risk particularly, but not only, in countries where institutions are

[23] This was also advocated by the US Fed in "detecting synthetic identity fraud in the US payment system" (FedPayments Improvements 2019). AI tools can help detect frauds in the Australian Medicare on many features outside of PIIs, or in credit card fraud detection (Tang and others 2011 and Alshammari and others 2022).

[24] Haksar and others 2021 emphasizes the increasing importance of personal data as a key input and source of value for companies across sectors. Koonprasert and others (2024) also discuss the incentives that central bank may consider providing intermediaries, to use CBDC data to build and charge for value-added services.

[25] Article 12 of the Universal Declaration of Human Rights and Art. 17 of the International Covenant on Civil and Political Rights prohibit arbitrary or unlawful interference with anyone's privacy and give individuals the right to protection of the law against such interference.

captured, and rule of law is weak. Notably, data collection and sharing could be a new step for central banks which might not have sufficient experience or skills. Data abuse could lead to invasive marketing, discrimination, or manipulation of consumer behavior. If CBDC transactions involve third parties that have commercial interests, arguably, there is an even greater risk that these entities could mishandle or misuse the data.

- **Cyberattack.** The CBDC ecosystem could become targets for cyberattacks, such as hacking, phishing, and malware. These attacks could steal user's personal data or disrupt currency operations. Cyberattacks can compromise the integrity of the financial system, lead to financial losses for consumers, and significantly undermine confidence. Potential risks could stem from the advent of quantum computing, vis-à-vis the many non-quantum-proof cryptography already deployed in existing payment and web systems (although CBDC could be designed to be quantum-proof from the get-go). Resilience to cyberattack is therefore an important factor in building trust in CBDC, as any successful attack or data breach could erode public trust and confidence with systemic implications.[26]

- **Cross-border data flows.** If CBDC is used for international transactions, data may flow across borders. This can complicate privacy protection due to varying data protection laws and the potential for individuals' personal data to be transferred (without their informed consent) to countries with lower data protection standards, which can also result in unauthorized access to the data used for foreign government surveillance. There are risks associated with jurisdictional control over the data, potentially exposing users to international data breaches (Annex IV).

Risks to privacy could be costly and undermine public trust. Insufficient mitigation of privacy risks can be costly for consumers, from tangible costs such as identity theft or discrimination to fewer tangible ones such as stigma or psychological discomfort (Acquisti, Taylor, and Wagman 2016). The costs associated with inadequate privacy protection are substantial, as evidenced by the fact that in 2021, around 15 million consumers in the United States were impacted by identity theft, causing losses of approximately US$ 24 billion (Javelin 2022).[27] In addition, risks to privacy could undermine public trust in CBDC. For instance, the largest group of respondents (41 percent) chose privacy protection as the most important characteristic to consider when issuing a CBDC (ECB 2021).[28] Privacy is one of the key issues for a potential US CBDC (Board of Governors of the Federal Reserve System 2022).[29]

[26] For more discussion of these topics, see Section 5 "Tools for Managing the Trade-off between CBDC Data Use and Privacy Protection" and Fintech Note on "Cyber Resilience of the CBDC Ecosystem" (Bharath, Paduraru, and Gaidosch 2024).

[27] Identity Fraud Losses Total $52 Billion in 2021, Impacting 42 Million U.S. Adults | Javelin (javelinstrategy.com)

[28] Eurosystem report on the public consultation on a digital euro (europa.eu).

[29] Money and Payments: The U.S. Dollar in the Age of Digital Transformation (federalreserve.gov)

4. A Framework to Navigate the Trade-off between CBDC Data Use and Privacy Protection

This section offers a framework for countries to manage trade-offs between CBDC data use and privacy protection. It draws on insights from the economics of data and privacy and discusses the role of design choices, principles and policies, and technology, in allowing countries to improve the trade-off. At the heart of the framework is the need to address externalities that may exist in CBDC data use, and to shape the incentives of the stakeholders in the CBDC ecosystem.

The trade-off countries face in managing CBDC data use and privacy protection depends on what data is required for achieving policy objectives—aggregated[30] or personal data; and if personal data, which specific personal data generated by CBDC. Processing aggregated data would not generally lead to privacy concerns,[31] but disaggregated personal data could. There could be a possibility of privacy being invaded to a degree that exceeds what consumers are willing to tolerate. If only aggregated data are required to derive, for example, social value, then there would be no (or minimal) trade-off with privacy. For personal data, the trade-off could relate to data-based innovation and growth, private or social value versus the desire of the individual to keep their data private.

The economics of privacy argues that effective privacy is about giving individuals control over their personal data. Privacy should not be understood as preventing the sharing of personal information, but rather as giving data subjects control over access to their data (Acquisti, Taylor, and Wagman 2016). According to Haksar and others (2021), when individuals are unaware, or do not have a say when it comes to the use of their data, an externality results: “decisions by companies about whether to collect, process, or share personal data can harm the individual who may not be compensated. These externalities are often negative, with the data used for instance to charge the individual a higher price, and this leads to too much data on individuals being collected and processed.”

At the same time, the economics of data shows that society will get more benefits from the data it generates when it is made widely available to many data processors (Jones and Tonetti 2020). The allocation of value from higher efficiencies will depend on competition and the market power enjoyed by individuals and data processors. When a data processor has collected data valuable to its commercial interests, there is a strong private incentive to hoard that data and withhold it from competitors.

[30] Data can be anonymized and grouped to allow for publication and circulation. Payment statistics can provide information on the overall number and value of payment transactions, as well as for the type of payment instrument and service. Such data can be used for analysis, oversight, and research purposes. See, for example, payment statistics (europa.eu).

[31] While aggregated data can be anonymized, individual market players could still be identified if they have significant market share or asset size.

Data use and privacy protection are also intrinsically linked to trust, and trust is the very foundation of money. Sufficient information needs to be provided in order to build a lasting and sustainable trust network to facilitate money flows (Adrian and others 2023). On the one hand, the holder of a CBDC needs to trust the issuer (even in a central bank–issued currency given this is a liability of a government)—that the CBDC ecosystem is secure and their claim is legally sound (including across multiple jurisdictions if used cross-border). On the other hand, the issuer must, in turn, trust the CBDC holder who must satisfy AML/CFT and other compliance rules. This trust can be expensive to build but at the same time cannot be constructed to the detriment of privacy, as privacy is also inherent to the nature of money (Kahn, McAndrews, and Roberds 2005).

Central banks can help build this trust by making public commitments to being transparent and accountable for CBDC data use. Several central banks have already made public declarations in relation to domestic CBDC data use, including the ECB and Bank of England.[32] Another way to increase transparency is to consider the desirability of open-source code on how CBDC data will be accessed by the central bank.[33] Commitment to being transparent can also allow for the cross-border sharing of CBDC data. For example, GDPR requires an "adequacy decision" for cross-border data use. That is, other jurisdictions must have a similar level of data protection for transfer of personal data outside of the EU. Therefore, a legal extension of trust can be built between jurisdictions.

Balancing the trade-off between public good that can be achieved with data sharing and use and the potential harm to individuals is central to effective data governance (OECD 2015). The extent of privacy regulation should represent a trade-off between the benefits of data-based innovation and the harms caused by violations of consumer privacy. It is important for regulators to balance consumer uneasiness with data collection and usage and with the consequences such regulations may have on certain types of innovation.

Managing the trade-off between CBDC data use and privacy protection also requires setting the right incentives for the stakeholders in the CBDC ecosystem. Stakeholders in the CBDC ecosystem are likely to have different objectives and responsibilities. Consumers and merchants would likely request personal data and privacy protection, while PSPs, central banks, and regulators should provide this protection (Table 3). Moreover, the design of CBDC may face a principal–agent problem, as PSPs are central banks' agents, but they may not be as careful or motivated to treat CBDC data and privacy issues as the principal—the central bank—would like. This principal–agent tension could result in higher risks to privacy; thus, it is important to put in place institutional safeguards and policies, as well as laws, that will ensure that the PSPs protect privacy properly.

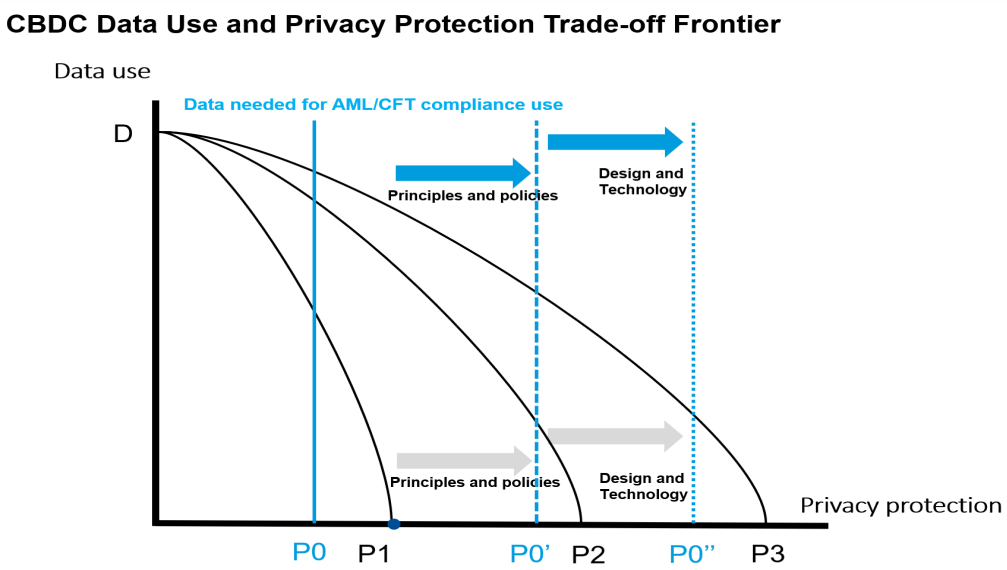
[32] See footnotes 17 and 18.

[33] For instance, the Banco Central do Brasil has a GitHub repository with documentation, which provides examples of use cases and open-source code on their Digital Real pilot for public audit https://github.com/bacen/pilotord-kit-onboarding.

Table 3. CBDC Stakeholders, Data Use, and Privacy Protection			
	Data Use and Privacy Protection		
Stakeholders	Aggregated Data	Personal Data	Privacy
Consumers	No use	Use (for control)	Demand for protection
Merchants	Use (for business development)	Use (for business development)	Demand for protection
PSPs	Use (for business development)	Use (for business development)	Supply of protection
Central banks	Use (for monetary policy and other macro objectives)	No use	Supply of protection
Regulators	No use	Use (including for AML/CFT)	Supply of protection
Source: Authors.			

Central banks are likely in a good position to manage the externalities and incentives in CBDC data use and privacy protection through a variety of policy instruments and tools. They may do so by offering a rich menu of design choices to cater to different preferences for privacy, and by adopting rigorous institutional safeguards and policies and innovative technological solutions. Indeed, the trade-off frontier between data use and privacy protection may be shifted to the right by a judicious use of policies, design choices, and technologies (Figure 2). Personal data can be protected through regulation that reflects adequate data protection principles and policies, through the design of the CBDC and by use of privacy enhancing technology. These tools are explored in more detail in section 5 “Tools for Managing the Trade-off between CBDC Data Use and Privacy Protection.”

Figure 2. The Privacy Protection Trade-off Frontier[34]



Data use necessarily impedes on privacy, hence the D – Ps arcs to illustrate this trade-off. However, various tools could push the frontier of what is feasible. Dedicated *principles and policies* could extend the trade-off frontier from the D - P1 arc to the D - P2 arc. Careful *design and relevant use of PETs* could push the trade-off frontier further, from the D - P2 arc to the D - P3 arc.
Similarly, AML/CFT data requirement *(represented as a line at P0)* can be made to better protect privacy with the same tools, as represented by the shift from P0 to P0' and then further to P0''.

Source: Authors.

Additionally, compared with the private sector, central banks may have several advantages in striking a balance between CBDC data use and privacy protection. Central banks as public institutions have no interest in profiting from payment data, unlike private sector providers as highlighted by the ECB.[35] Central banks could strengthen communication and education to reduce privacy concerns. As consumers are often in a position of imperfect or asymmetric information, central banks can better communicate and educate consumers. These will help reduce discrepancy between attitudes and behaviors.

Central banks may have more resources and capacities to coordinate on data and privacy policy to promote innovation and competition. For instance, central banks could also coordinate with other regulatory agencies to avoid too much privacy regulation that could hamper innovation. This will help small and new firms to be compliant with privacy regulation and mitigate the prevalence of "walled gardens," thus avoiding giving large firms an advantage over small firms.[36]

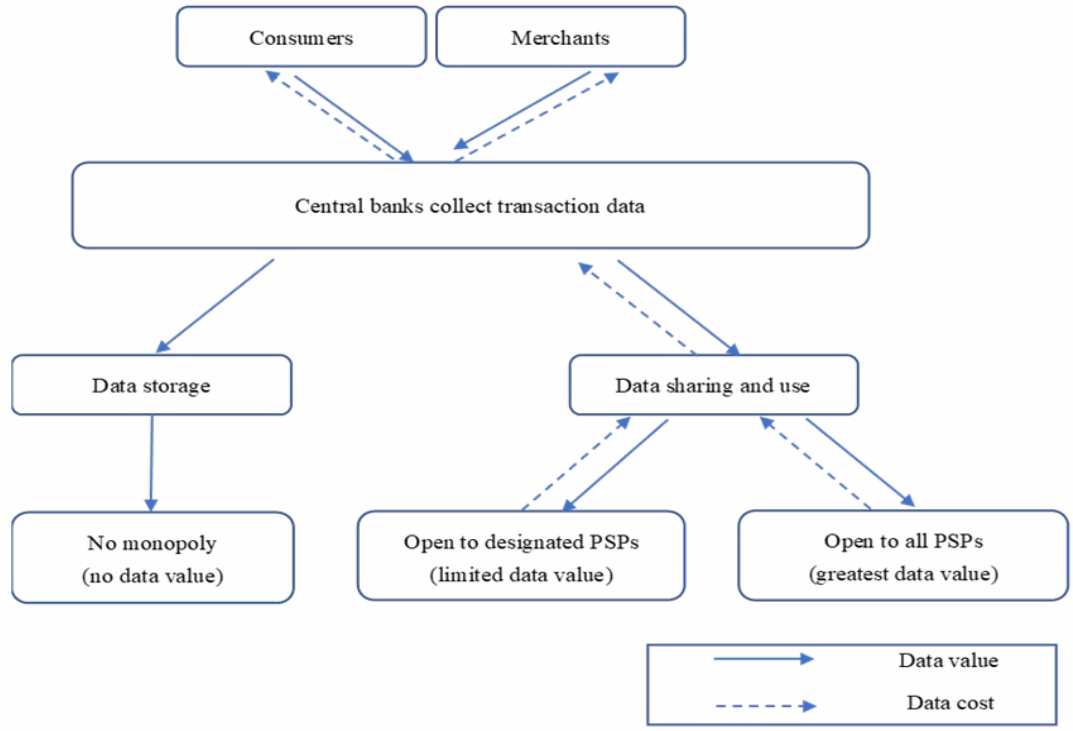
[34] The figure intends to describe the trade-off between privacy and data use value, as well as how policies, design, and technology could shift the trade-off. The horizontal axis shows the degree of privacy protection, the further to the right, the higher the protection. The vertical axis shows the extent of data use, the further to the top, the more data use. More PETs and better design and policies can extend the frontier of data use while keeping the same level of privacy protection, hence allowing a better data use versus privacy trade-off.

[35] See ECB blog, Making the digital euro truly private (europa.eu).

[36] Privacy regulations may facilitate the prevalence of "walled gardens" on the Internet, because consumers have a difficult time understanding privacy notices in the absence of standardized language (Kelley and others 2010), thus giving large firms an advantage over small firms.

Central banks could use CBDC to address the data silo problem to further enhance competition. Central banks may be able to establish a clear data-sharing arrangement and discourage PSPs from withholding investments in creative data-driven business models. The sharing of CBDC data, based on consent, can help integrate CBDC into existing payment systems (for example, BigTech ecosystems), break data monopolies, and harness the economic value of data regardless of whether the CBDC is a one-tier or two-tier model (Figure 3). Central banks can require all PSPs to share data in a platform and encourage PSPs to use the data. However, central banks have to make an important policy decision regarding whether they would share data so that PSPs can use that data.

Figure 3. Data-Sharing Arrangements



Source: Sun and Rizaldy (2023).

Note: Central banks could either collect transaction data from PSPs (in a two-tier model) or by itself (in a one-tier model). Data value refers to the harnessing of the economic value of data by PSPs. Data cost refers to the cost PSPs would incur to protect privacy if central banks are able to establish clear data-sharing arrangements.

5. Tools for Managing the Trade-off between CBDC Data Use and Privacy Protection

This section discusses how to protect privacy of personal data through the establishment and application of principles and policies that are reflected in regulation, through privacy-by-design and by using privacy enhancing technology to manage the trade-off described under section 4 "A Framework to Navigate the Trade-off between CBDC Data Use and Privacy Protection."

CBDC data use and privacy protection must adhere to the principles of existing and emerging data frameworks. They must be consistent with privacy protection laws, consumer protection laws and applicable central bank laws. Privacy protection could even be included in the constitution of a jurisdiction. Principles and policies have to be considered jurisdiction specific. CBDC data allows for commercial exploitation while also raising the possibility of state surveillance. Whether populations place greater trust in their government or in commercial bodies would be an important factor. Tucker (2023) points out commercial and government surveillance are not equal given firms cannot confiscate property or send someone to jail.

Empowering individuals by giving them greater control over the processing of their personal data, with the assistance of laws and policies, would help build public trust and influence individual behaviors. Acquisti, Brandimarte, and Loewenstein (2015) suggest policy approaches that focus on education or "empowering" individuals are unlikely to offer sufficient protection against privacy risks. Instead, they propose the goal be to achieve a more even equity of power between consumers and governments/ institutions, which generally have the upper hand in this regard.

PSPs and central banks should be subject to the country's data protection laws when processing personal data in relation to CBDC and should be supervised by the relevant authorities. Both PSPs and central banks should put in place processes and procedures to ensure compliance with the data protection laws.

Data Protection Legal Frameworks

Discussions on data protection focus on how to implement or adapt data protection legal frameworks to CBDC. Data protection legal frameworks generally uphold the principle that an individual has the "right to determine what information is collected on [him/her/them], how it's stored, and what it's used for."[37] Several countries, regional and international bodies[38] (Box 1), and supranational organizations (such as the EU, Box 2) have adopted rules on data protection that typically have broad provisions and principles

[37] Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," *NYU Review of Law and Social Change* 42 (2018) 253-307.

[38] Examples include the Asia-Pacific Economic Cooperation (APEC) Privacy Framework; the Association of Southeast Asian Nations (ASEAN) Framework on Digital Data Governance, and ASEAN Framework on Personal Data Protection; the African Union Convention on Cyber-Security and Personal Data Protection; the Commonwealth of Nations Model Bill on the Protection of Personal Information, and the Model Privacy Bill; the Council of Europe's Modernized Convention on the Protection of Individuals with regards to Automated Processing of Personal Data (Convention 108+); the Caribbean Community's Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR) Privacy and Data Protection Model Policy Guidelines and Legislative Text; the Organization of American States' Updated Principles on Privacy and Personal Data; and the OECD Privacy Framework.

specific to personal information.[39] As these protections vary from jurisdiction to jurisdiction,[40] comparing CBDCs that are considered in various countries requires an understanding of their own data protection legal frameworks. A country considering the use or design of CBDCs should begin by understanding what, if any, data protection laws it already has in place, and what other data protection laws persons located in its territory need to comply with.[41] Other parts of a country's legislative framework, such as AML/CFT laws and regulations, as well as industry-specific laws applicable to banks and other institutions that could act as CBDC PSPs in a CBDC transaction, will also impact the fundamental design of a CBDC.

Box 1. International Data Protection Legal Frameworks

The first international data protection principles were set out in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data that were adopted on September 23, 1980, and revised on July 11, 2013 (the "OECD Privacy Guidelines").[42] "Since their adoption, the OECD Privacy Guidelines have been widely disseminated and implemented. OECD countries adhering to them repeatedly refer to the OECD Privacy Guidelines as forming the bedrock of their own national frameworks, and they are widely recognized as forming the basis of other data protection frameworks—demonstrating their global reach."[43]

The first international data protection principles were set out in the OECD Guidelines' first binding international instrument which protects individuals in relation to the processing of their personal data was the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data that was adopted on January 28, 1981, and subsequently signed by all 44 members of Council of Europe and 11 other countries.[44]

The scope of privacy protection available under the legal frameworks of individual countries and regions depends on the priorities of their governments and ultimately this may have a direct impact on consumer trust in CBDCs. The extent to which central banks and PSPs are transparent and clear about how they collect data and apply the relevant data protection legal framework can also impact trust. Since various legal frameworks differ both in terms of form and substance, an effective tool for analyzing and comparing those frameworks can be the underlying privacy principles. Four principles have been identified that contain legal requirements that are particularly relevant for privacy protection in CBDC transactions.

[39] The activity regulated by GDPR is referred to as "processing" and, as per the definition in Art. 4, it captures "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[40] See Annex IV of this paper on cross-border considerations and approaches.

[41] For example, as per Art. 3, GDPR applies to organizations located outside the EU that process personal data of EU residents and offer them goods and services. This means that, due to the size of the EU market, a large number of companies located outside of the EU comply with GDPR.

[42] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, Annex, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[43] See Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, p. 4.

[44] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

Privacy Principles

Central banks need to make sure that all processing of personal data generated by CBDCs is carried out in accordance with the privacy principles. The following four principles, established under the GDPR[45] and now widely accepted, are particularly relevant for CBDCs:

- **Integrity and confidentiality.** Personal data must be processed in a manner that ensures appropriate security including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage of data. In a CBDC context, the party or parties who are data controllers will have to implement robust information security standards and will also have to set up processes that will enable it to satisfy itself that any data processors participating in the CBDC transactions also comply with adequate information security standards.
- **Purpose limitation.** Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In a CBDC context, this means that the central bank, and any other party acting as the data controller, must be clear from the beginning of a CBDC transaction about what personal data it collects and what it intends to do with it (for example, to execute payment transactions) and whether it should reflect that in the relevant privacy notices. It should be noted that a certain amount of personal data is also necessary for regulatory purposes, and this should be taken into account when determining purposes of processing (including mitigating the abuse of the financial system).

- **Data minimization.** The amount of personal data processed should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Applying the data minimization principle to a CBDC would entail ensuring that in each phase of a CBDC transaction processing of personal data is limited to what is necessary to achieve the purpose of that phase. This is why it is crucial that the authorities designing CBDCs think carefully about what personal data a central bank or a financial intermediary or a law enforcement agency really needs to complete its task and achieve the purpose for which it is processing personal data. For example, sensitive data such as data on racial or ethnic origin, political opinion, religious beliefs, or medical data in most cases will not be needed at all and should not be collected.

- **Storage limitation.** Personal data should not be kept longer than what is needed for the purpose for which it is processed. If personal data are kept for longer than necessary, it is likely that retaining such data will not be lawful. Data controllers in a CBDC context will need to think about and justify the duration for which personal data are kept for example, through a policy that sets retention periods. This may be difficult to reconcile with the indefinite data retention that can occur on a blockchain as highlighted in a response to the Bank of England's CBDC consultation.[46]

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR) (europa.eu).

[46] response-to-the-bank-of-england-and-hm-treasury-s-consultation.pdf (ico.org.uk).

Another important privacy principle is lawfulness. Pursuant to GDPR,[47] a lawful basis should exist for processing personal data and it can be: (1) consent from the individual whose personal data are processed; (2) compliance with a legal obligation for which processing is necessary (for example, AML/CFT or tax or audit purposes); (3) performance of a contract to which the individual is party and for which processing is necessary; (4) protection of a vital interest of the individual or another natural person; (5) pursuing of legitimate interests for which processing is necessary and such interests are not overridden by interests of fundamental rights and freedoms of the individual that require protection of personal data; or (6) performance of a task carried out in the public interest or the carrying out of an official authority vested in the controller. Under the OECD Privacy Guidelines, for example, a similar purpose is achieved through the collection limitation principle, which among other requirements includes a requirement for personal data to be obtained by lawful means and, where appropriate, with the knowledge and consent of the data subject.[48]

Other privacy principles include fairness, transparency, and accuracy.[49] Fairness requires that personal data are not processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected, or misleading to the data subject.[50] Transparency requires that the individuals are informed in clear, plain, simple language about the lawful basis for processing of their personal data, for example in a privacy notice that is easily accessible in the central bank website. The notice would have to also include information about any third parties to which the central bank may transfer personal data and with which the CBDC holder may have no direct contractual relationship. Accuracy requires that personal data should be accurate and to be kept up to date. Those that process personal data must take reasonable steps to ensure that inaccurate personal data is erased or rectified without delay. CBDC holders would have to be given the right to access their personal data as well as to request corrections to be made to such data.

[47] Article 6(1) of the GDPR.

[48] OECD Privacy Guidelines, para. 7.

[49] Article 5(1)(a) of the GDPR.

[50] EDPB Guidelines on Data Protection by Design and by Default, p. 17, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

Box 2. GDPR and CBDC

EU's General Data Protection Regulation (GDPR) and its principles, discussed in the previous sections, provide a good reference point for starting a discussion on personal data protection in the context of CBDC. The following issues should be considered when applying these principles to a specific CBDC transaction:

- Who are the parties in a CBDC transaction and who among them has the main responsibility toward the individuals for ensuring that their personal data[51] are processed in accordance with the privacy principles? Such parties are referred to as the data controllers.[52] The responsibilities of the data controllers include ensuring that any other parties to whom they transfer personal data for processing, which are referred to as the data processors, also process personal data in accordance with the privacy principles. In the CBDC context, the individuals whose personal data are processed will be the payer and the payee and the parties that will have to be assigned the role of the data controller or the data processor will be the central bank, commercial banks, other intermediaries, such as mobile operators, nonbank PSPs, law enforcement agencies, financial supervisors, and authorities managing digital IDs. The role assigned to each of the parties will determine the scope of their obligations.
- What personal data are processed and through which processing activities? In the CBDC context, the personal data processed could include payers' and payees' names, the balances on their accounts or wallet addresses, where and when they made the payment, purpose of payment, and the monetary amount transferred. Processing activities include collection, storing, transmission, and deletion of personal data. Other personal data that may be linked to the CBDC context should also be considered such as when digital ID is used as a means of identification for onboarding CBDC users.

Modern privacy protection laws also build on fair information practices originated in the early 1970s at the United States Department of Health, Education, and Welfare. They were based on five principles: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress (United States Federal Trade Commission (FTC) 1998).[53] These principles became the basis of later guidelines and laws on privacy and personal data governance, including the Federal Trade Commission's effort to "encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online (FTC 1998)" and the EU Data Protection Principles Directive, the GDPR, and the California Consumer Privacy Act (CCPA) (Chen and others 2021).

[52] Article 4 of GDPR defines the term "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

[53] https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

CBDC Data Use and Privacy Protection Policies

Following the principles discussed earlier, a nuanced approach—dynamic and tailored to specific markets, contexts, and scenarios—may be necessary. Different stakeholders—including merchants, PSPs, consumers, and governments—may have different, multilayered, and often conflicting objectives, with no single policy being able to achieve a better trade-off. For instance, some countries and regions, led by the EU, have focused on establishing general principles that govern use of data across multiple sectors as shown in GDPR. It provides a very broad scope and stricter standards in comparison to other country or jurisdictional data governance laws. The United States has taken a more limited approach to privacy regulation, and consequently regulation has varied across industries and states (Goldfarb and Tucker 2012b). Given these potential diversities, the authorities should:

- Decide what data can be collected, stored, shared, and used; define the roles and responsibilities of all parties involved in the CBDC ecosystem regarding data access and usage; and take data protection measures, such as data security and encryption.
- Decide who is responsible and held accountable for ensuring that the privacy principles are being followed. For instance, bank supervisors should make sure that the Board of Directors of the PSPs are held accountable for setting up processes and implementing policies of privacy protection.
- Set up institutional mechanisms to ensure that established principles and policies for privacy protection are implemented, stakeholders are compliant, and violators are held accountable.
- Use the traditional tools for privacy protection tools such as choice, consent, control, and transparency to provide adequate privacy protection.
- Communicate with the public to provide information and transparency on the implications of different CBDC design choices for privacy.
- Offer a rich menu of CBDC designs to cater to different users and different preferences for privacy: from mostly anonymous wallets for small value transactions to full identity wallets for larger value transactions. Central bank can offer from low data intensity (with high privacy protection requirements) to high data intensity designs (with less privacy protection requirements).
- Decide how to convince the public that the central bank will not have access to CBDC data, if that is the choice of the central bank, depending on its own legal and regulatory practices.

Privacy-by-design Philosophy and CBDC Design

The privacy-by-design philosophy advocates for organizations to consider privacy at the initial design stages of projects. It applies to the complete development process of new products, processes, or services that involve processing personal data. It is a comprehensive and holistic approach to protecting privacy by embedding privacy protection into design, business practices, and infrastructures from the outset. It could help implement privacy protection principles and policies.

The framework is founded on seven principles. It promotes a proactive and anticipatory approach to privacy (principle 1), ensuring that privacy safeguards are embedded within systems as default settings, thereby obviating the need for users to undertake additional steps to protect their privacy (principle 2). The importance of robust end-to-end security is underscored, ensuring that personal data remain protected throughout its entire lifecycle from collection to disposal (principles 3 and 5). Moreover, this seamless integration of privacy within the design should not compromise its functionalities; rather, privacy-by-design aspires to a win-win situation where privacy and data utility coexist, each unimpeded by the other. This principle challenges the notion that privacy and security must be traded off against one another, advocating instead for solutions that satisfy both objectives (principle 4). Additionally, the framework champions visibility and transparency, enabling users and stakeholders to verify compliance and the integrity of practices (principle 6), complemented by clear education and messaging, and features putting users at the center (principle 7).

Privacy-by-design encompasses eight distinct strategies, delineated as “minimize (data collection), separate (data storage), aggregate (when using data), hide (PIIs), inform (users), (offer users) control over their data, enforce (legal requirements), and demonstrate (compliance with privacy principles and laws)” (Hoepman 2014). For each design strategy, specific PETs can be employed. The basic strategy is to limit the collection and processing of personal data to the strict minimum necessary. Additionally, data producers, such as PSPs, could be under certain circumstances required to secure authorization from users prior to collecting personal data and to anonymize this data using pseudonyms before its analysis and utilization. In the context of CBDC, central banks have the opportunity to design and deploy software that enables PSPs to offer privacy protections or provide interfaces that enhance users’ understanding of the privacy clauses and the extent to which technologies safeguard their sensitive information (Rubinstein and Good 2013). Finally, the retention period that the personal data is held by the central banks and/or PSPs might need a policy decision, which could impact design choices and other components of the privacy-by-design framework.

Privacy Enhancing Technologies (PETs)

PETs comprise a broad range of software and methodologies designed to protect users’ personal information and maintain the confidentiality of their online activities. These technologies aim to minimize or eliminate the collection and dissemination of personal data, thus preserving privacy.

PETs are often deployed as a way to implement a privacy-by-design philosophy. Given the varied contexts, different PETs, such as zero knowledge proof (ZKP), can be used to conceal information held by a single entity (for example, identities or account balances) and multiparty computation (MPC) to obscure inputs into a common computation (like in a smart contract). These two families of technologies also provide mathematical guarantees that no other information than those intended can be learned, ensuring that any attempt to deviate from the protocol can be detected (so-called proof of correct execution).

PETs are also applied to address specific challenges. Anonymization techniques, encompassing various data anonymization methods such as *k*-anonymity and differential privacy, are designed to prevent the identification of individuals from datasets. Access control and consent management, as privacy protection

technologies, allow users to manage data access permissions and purposes, like privacy settings on social media platforms. PETs can either improve or impede policy implementation. Although being potentially used in a CBDC context to prevent unauthorized access to personal data, PETs have also been used in the context of crypto assets to facilitate illicit activity and challenge supervisory and law enforcement efforts.

CBDC offers opportunities to deploy PETs from the beginning, as it is a "clean slate" built on new institutional arrangements, legal frameworks, and technologies. Central banks would have incentives to deploy PETs early on if they aim to strike a good balance between CBDC data use and privacy protection. CBDC can be designed to introduce a possible segregation of data lifecycle phases into distinct engineering modules and roles, allowing for the protection of each module and role with various layers of technology. This ensures that privacy domain of different modules and roles do not encroach upon each other. Therefore, different technologies and modules could be leveraged to protect privacy. However, institutional arrangements and legal frameworks are needed to complement technology by preventing misuse of technology and ensuing transparency and accountability in data management.

Three examples can be used to illustrate how PETs can be deployed in CBDC design (Annex V). The first example shows that PETs make it possible for the CBDC ecosystem to comply with AML/CFT requirements without the central bank accessing any personal identity information.[54] This is done by, for instance, institutionally separating operators that are responsible for AML/CFT compliance (for example, PSPs) from other operators, so that the central bank can only see aggregated, anonymized, or otherwise sanitized data. Proofs can be generated on what information was used in what operations. The second example shows that various cryptographic solutions could be deployed to conceal some transaction data from PSPs if CBDC users prefer not to allow the transaction data to be used by PSPs for commercial purposes. The third example shows how PETs can help safeguard privacy when computations are needed over granular transaction data, while still masking and protecting personal data. These computations can be for example those building aggregate measures for macroeconomic analysis and policymaking. The setup of trusted third parties in charge of anonymizing personal data is a first institutional solution, to be further fortified by the identity operators to issue multiple "pseudo-identities" for different transaction purposes to mask individual identities when these transactions are being aggregated. Finally, the same type of proofs on what information was used in what operations could be audited and communicated to build trust in CBDCs.

Central banks could collaborate with private sector and academics to explore and scale up PETs. PETs are in a relatively early stage of development and are mostly confined to the academic realm. PETs require development skills and resources. They also require the private sector to have incentives to develop and apply PETs. Central banks are in a better position to deploy PETs more extensively than the private sector if they are mandated to enhance privacy protection while allowing use of CBDC data. For instance, several projects coordinated by the BIS Innovation Hub, such as Project Tourbillon, Project

[54] In China, for example, a guideline for e-CNY on AML/CFT has been published and deployment of supervisory technology (SupTech) has been strengthened.

Aurum 2.0, and Project Hertha, demonstrate central banks' collaboration with private sector and academics to explore and scale up PETs.[55]

Cross-Border Considerations

Harmonization of regulatory standards and the use of technology can assist in safeguarding privacy while allowing cross-border CBDC data flows. Data need to be shared, for instance, for AML/CFT purposes, in order for cross-border payments to be made. While shared, they are subject to risks to privacy infringements which differ by jurisdiction.[56] The ability to transfer data is key for cross-border CBDC payments to function but data to be transferred differ depending on the payment corridor, the purpose of the transfer and the amount being transferred. Solutions can be found when interlinking CBDCs through use of PETs. How to strike a balance between cross-border payments data use and privacy protection is the subject of much discussion at international level by the Financial Action Task Force (FATF), the Financial Stability Board (FSB), G7, and the OECD among others. Agreements and actions taken by standard setting bodies, international organizations, and others will have an impact on cross-border CBDC data use (Annex IV).

[55] See Project Tourbillon: exploring privacy, security and scalability for CBDCs (bis.org), Mandala, Project Aurum 2.0: Improving privacy for retail CBDC payment (bis.org), and Project Hertha: identifying financial crime patterns while preserving user privacy within a real-time payment system (bis.org).

[56] All else equal, CBDC does not pose greater risks to privacy than legacy cross-border payment systems.

6. Conclusions

This Fintech Note analyzed how to strike a balance between CBDC data use and privacy protection in retail CBDC. How countries manage this balance and trade-off will depend on country-specific circumstances, their policy objectives (including those of their governments), and global standards. It recognizes that the appropriate degree of privacy in a CBDC system is a political and social question. While some countries will likely opt for a high degree of privacy in the design of CBDC and the central banks involved will choose not to give much weight to the economic value of CBDC data, other countries will likely take advantage of CBDC data use for certain policy objectives such as fostering financial inclusion and promoting competition in the payment systems.

Central banks may be well positioned to strike a good balance between CBDC data use and privacy protection as CBDC systems could start as a "clean slate." In designing CBDC, central banks may wish to offer a variety of CBDC privacy settings to cater to the privacy needs of different users. In setting up the CBDC ecosystem, central banks should focus on addressing externalities that may exist in CBDC data use, and on shaping the incentives of the stakeholders in the CBDC ecosystem.

This note outlines the tools that could help manage the trade-off through application of laws and regulations that reflect adequate privacy principles and policies, careful CBDC designs, and adoption of the privacy-by-design philosophy and judicious use of PETs. Data use and privacy protection do not have to constitute an insurmountable trade-off. There should be less of a trade-off if the right tools are used to reduce privacy concerns and encourage consumers to be more willing to share and use personal data, knowing that such data are sufficiently protected.

Annex I. Potential CBDC Use in Monetary Statistics

CBDCs introduce a new form of central bank money, which need to be accommodated within the measures of monetary base and overall money supply, central concepts in monetary statistics. Irrespective of the type or design—whether account-based- or token-based—CBDCs are a central bank liability and a component of monetary base.

An important feature of macroeconomic statistics is that even when personal data are used as a source the anonymity of private individual information is always preserved. The use of CBDC-related personal data, aggregated to the subsector or sector level, would not affect privacy but rather would provide the central bank the possibility to gather information on CBDC holdings by money holding and neutral sectors, thus improving the quality of estimating monetary base and related money supply in the economy.

Higher level of granularity coming from aggregated CBDC-related personal data, of which the holder's sector and location (domestic region and country), brings more depth within monetary statistics and liquidity aggregates in the event of currency substitution to meet policymakers' needs. In addition to sectoral breakdown, geographical aggregate views of CBDC transactions could enable policymakers to monitor the transmission of economic shocks within the domestic economy in real time as well as cross-border spillovers. Even though both CBDCs and cash are direct claims on the central bank, CBDCs have different attributes to cash, as it may be possible to know the holders in real time and even to program payments. The availability of micro-level high frequency data associated with CBDCs may thus provide more insight to central banks for better informing monetary policy decisions and understanding the transmission mechanism.

In the absence of strong regulation on usage, should residents in one jurisdiction be allowed to use foreign CBDCs, access to CBDC-related personal data (particularly on counterpart holders) can be valuable to address policy challenges stemming from currency substitution. Concerns over currency substitutions are not new. The effective design of CBDCs based on digital ID and implemented as an account-based system can be expected to largely eliminate such risks. In that respect, central banks, both the issuing and the recipient one in another jurisdiction, are cognizant of the risks.

Comprehensive information available on financial transactions in CBDCs between different parties (including cross-border) from the payment system also mirrors underlying economic transactions and is beneficial in informing country authorities about the propagation of any underlying economic shocks and cross-border spillovers. For instance, changes in payments patterns drawn from detailed information on CBDC-related personal data can show real-time information on the nature and impact of an economic shock—be it demand, supply, structural, or external. Also, the transaction between a payer and a payee

through the payment system in domestic/foreign CBDC may disclose a resident/nonresident transaction on a tourist travel in a domestic/foreign destination.

Annex II. The G20 Data Gaps Initiative-3 and CBDC

The G20 Finance Ministers and Central Bank Governors in November 2022 welcomed the new Data Gaps Initiative-3 (DGI-3), which, among others, addresses priority policy needs related to financial innovation.

Recommendation 11 on digital money within the DGI-3 focuses on CBDCs among other digital payment instruments and serves as a foundational step in standardizing the approach to collecting, analyzing, and sharing data related to CBDCs. Within the framework of Recommendation 11, key outcomes include the development of a common data template and accompanying guidance on data collection, including CBDCs.[57] More broadly, Recommendation 11 seeks to spark a discussion among G20 economies about the macroeconomic data requirements in a future where CBDCs and other digital payment methods are widely used both domestically and across borders. It also aims to facilitate a more robust framework for data sharing among countries, beginning with the G20 economies.

Central banks issuing CBDCs can use personal data to meet these data requirements through the design features that enable the identification of the CBDC holders' institutional sector, and the location (counterpart country). Alternatively, in a two-tier model, central banks, through domestic legislation, may require PSPs, such as banks and other intermediaries within the CBDC value chain, to gather information about the institutional sector of CBDC holders (for example, households and nonfinancial corporations), and country of residence.

Recommendation 11 also recognizes the challenges that arise should foreign CBDCs gain widespread adoption in a host economy. The common data template, a central component of Recommendation 11, will not only ensure comprehensive coverage of CBDCs in monetary statistics and international capital flows measurement but also account for data needs across different jurisdictions. It will encompass dimensions related to resident and nonresidents (as defined in international statistical standards).

[57] The goal is to have preliminary estimates of CBDCs available by the fourth quarter of 2025.

Annex III. BigTech Payments and Privacy—Are There Lessons for CBDC Design?

Over the past two decades since Alibaba launched Alipay in China, several major tech companies (BigTechs) have come to offer digital means of payment and in some cases also provide credit ratings derived from payment data. This annex considers whether there are lessons to be drawn from their experiences for CBDC design, including its potential implications on privacy.

Market power is a key facet that differentiates a digital payment system dominated by a BigTech provider from a payment system centered on bank deposits. In the latter, competition between banks sets bounds on the market power (for example, in lending), which a bank derives from its depositors' payment data. However, with the rise of BigTechs, payment data has been migrating out of banks' hands. Even if a household uses a bank-issued card to pay on a BigTech's platform, the payment details of what has been bought are in the BigTech's hands. When a BigTech issues a digital means of payment that gains widespread use, it also obtains data about transactions outside of its platform. In addition, a BigTech often possesses granular nonpayment data on households from its ecommerce or social media platform.

On the one hand, there is growing evidence that BigTech-issued means of payment can help expand credit access. For instance, in some countries previously unbanked borrowers have been able to leverage their digital payment trails to gain credit inclusion (see the literature cited in Agur, Ari, and Dell'Ariccia 2023). On the other hand, when pairing their data troves with credit provision, BigTechs have profit incentives to erode consumer privacy. When households choose which means of payment to use for consumption, their personal preferences for privacy play a role. However, a key insight from the literature on privacy in payments is that privacy is more than just personal and has elements of a public good. As Agur, Ari, and Dell'Ariccia (2023) show, a BigTech can box households into using its payment system that dislike this.

The potential positive (inclusion) and negative (privacy) effects of BigTech payment structures may apply to CBDC, but this will depend on the structure of the PSPs that disseminate the two-tier CBDC. When there is a single PSP disseminating the CBDC and that PSP is a nonbank (and is allowed to collect and retain CBDC payment data), the resulting payment system could well come to resemble one dominated by a BigTech, because a nonbank that manages payment data is a central node in the economy that would have incentives to launch additional nonbank services or platforms tied to its central role. This would therefore be anticompetitive when CBDC data should ideally be used to promote greater competition.

The regulatory bounds on a commercial bank instead limit the types of activities it can engage in. In providing credit, a bank might use the payment data it collects but would be unlikely to gain access to a broader trove of nonpayment data in the manner of a BigTech. If multiple banks are appointed as the PSPs of the CBDC, the emerging structure would likely resemble the traditional payment system, where payment data is spread among competing banks thereby ensuring competition.

Finally, if multiple nonbank PSPs compete, the number of PSPs and the intensity of competition between them may determine if CBDC data are closer to one with the market power that is characteristic of BigTechs or more like a traditional bank-based payment system.

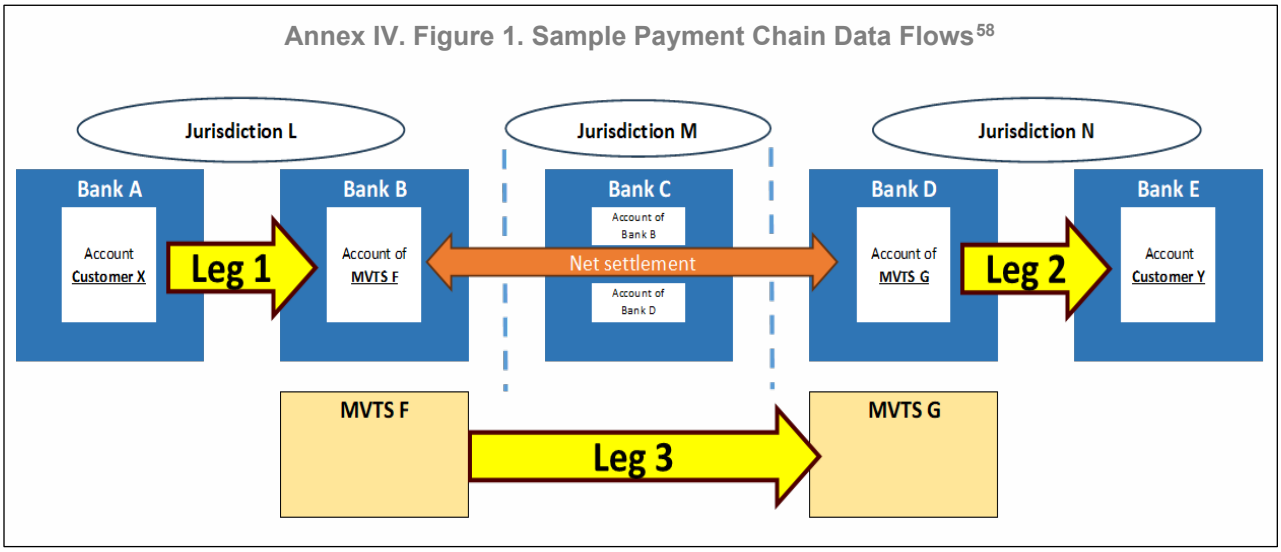
Annex IV. Cross-Border Considerations and Approaches

This section considers key challenges to data use and privacy protection when CBDC is used for cross-border payments. It then outlines policy initiatives in the global policy community to address those challenges.

Data need to be shared in order for cross-border payments to be made, including for regulatory purposes. While they are being shared, they are subject to risks to privacy infringement, especially as countries have different standards of privacy protection. At the same time, country authorities increasingly have more stringent requirements which may not be sufficiently coordinated and not conducive to striking an optimal balance between data use and privacy protection.

The ability to transfer data is key for the orderly functioning of cross-border CBDC payments. Data to be transferred depend on the payment corridor requirements, the purpose of the transfer, the amount being transferred and so on. These criteria determine what data need to be transferred. For instance, FATF Recommendation 16 discusses data transfer in a payment chain. Any required originator and beneficiary information should travel the entire length of the cross-border payments (Figure 4).

Annex IV. Figure 1. Sample Payment Chain Data Flows[58]



Cross-border use and sharing of CBDC data needs to be balanced with privacy protection. CBDC data need to be shared across borders for legal and regulatory, AML/CFT, sanctions screening, and information-sharing purposes. Yet, at the same time, protecting the privacy of users and their personal

[58] A money or value transfer service (MTVS) denotes "financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs" (FATF 2016). In this illustrative example and as described by the FATF Explanatory Memorandum and draft revisions to Recommendation 16 from February 2024, "Customer X with account at MVTS F, instructs the MVTS F to transfer funds from her/his account at MVTS F to Customer Y." "The start point is MVTS F. All required information therefore needs to be carried in the payment chain from MVTS F ⇒ MVTS G ⇒ Bank D ⇒ Bank E." Note that this text refers to draft revisions that are not yet finalized.

data is paramount to successful CBDC adoption. In addition, existing laws and regulations differ across jurisdictions and CBDCs are confronted with considerable fragmentation. The FSB has identified several sources of friction that would also be of relevance to CBDC data use and privacy protection (Annex IV. Box 1).

How to strike a balance between cross-border CBDC data use and privacy protection is the subject of much discussion. The G7 Public Policy Principles for Retail CBDCs encourage jurisdictions to work openly and collaboratively on international dimensions when designing CBDCs (G7 2021) and at the same time consider rigorous standards of privacy as being essential for any CBDC to command public trust and confidence. The European Data Protection Board strongly recommend that there should be a "privacy threshold" for online transactions under which offline and online value transactions are not traced for AML/CFT purposes. While this recommendation does not yet apply to cross-border transactions it could have implications for cross-border digital euro payments.[59]

The "data free flow with trust" (DFFT) concept, championed by Japan, endorsed by the G20 and the G7 and operationalized at the OECD, aims to promote free data flow while ensuring privacy, and other public policy objectives.[60] The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, adopted in December 2022, identifies common approaches to safeguard privacy and other human rights and freedoms when national security and law enforcement agencies in different countries access personal data—an important consideration for CBDC given the high desire in some jurisdictions for anonymity of transaction data.[61] The Declaration recognizes that law enforcement and national security authorities are vested with powers under national legal frameworks to lawfully access personal data. Such access is governed by the applicable national legal framework and therefore differs by jurisdiction.

Satisfying AML/CFT requirements may require customized privacy solutions. The CPMI proposed several solutions to this complex issue (CPMI 2022). Jurisdictions could propose thresholds to identify significant transactions for enhanced due diligence (as for the digital euro), as long as they adequately account for and can mitigate associated money laundering and terrorism financing risks. Multi-CBDC (mCBDC) arrangements could agree to a threshold approach, but it may be difficult to arrive at a single set of rules for countries with varying risk profiles, regulatory rigor, and capacity. Alternatively, a modularized design could be pursued which would allow for rules and functions to be customized to country needs.

The G20 Roadmap for Enhancing Cross-Border Payments contain several actions that will be helpful for CBDC data use and privacy protection (Annex IV. Box 2). The importance of data flows in cross-border payments is illustrated by cross-border data exchange and message standards being one of three priority themes under the priority actions. The G20 acknowledges that enhancing and harmonizing the data contained in cross-border payment messages, including through CBDC transactions, would assist in supporting straight-through processing, automated reconciliation, and effective AML/CFT controls (FSB 2023).

[59] See Digital euro: ensuring the highest data protection and privacy standards | European Data Protection Board.
[60] See OECD, Data governance.
[61] See OECD, Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access.

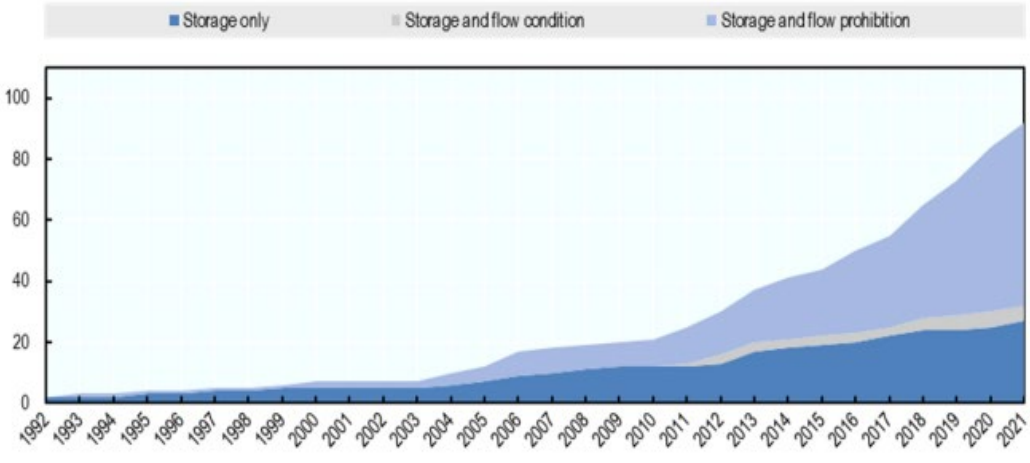
Annex IV. Box 1. Challenges for CBDC Data Use and Privacy Protection in Cross-Border Payments

The FSB, in their stocktake of international data standards relevant to cross-border payments, identified several sources of friction that would also be of relevance to CBDC data use and privacy protection (FSB 2023).

- **Fragmented data framework requirements.** In particular, what data are required to accompany an international payment is not standard across jurisdictions. There are jurisdiction-specific requirements for messaging and legal documentation as well as variations in implementation of FATF Recommendation 16: Wire Transfers.[62]
- **Restrictions on data flows.** Some jurisdictions require data to be stored or processed within that jurisdiction (data localization) which can have implications in terms of overhead, maintenance, security of data, and resilience. Data localization measures can hinder compliance with local regulatory and supervisory requirements.
- **Frictions that hamper innovation, such as CBDC.** With no global approach to data frameworks, innovation becomes more challenging if data use cross-border is limited and citizen's data privacy overrides the ability to transfer it.

Stringent data localization requirements have their potential to disrupt cross-border data flows and impose burdens on economies, especially developing ones (Haksar and others 2021). While data localization may enhance data sovereignty and security, excessively stringent requirements might hinder the growth of the digital economy by restricting the flow of data necessary for CBDC data use across borders (CRS 2023).[63] Exploring alternative measures like mutual recognition agreements or data protection standards that allow for cross-border data flows can mitigate the negative impacts of stringent data localization. This would support the seamless operation of CBDC data use across jurisdictions (Sai Rakshith Potluri, V Sridhar, and Shrisha Rao 2020).[64] Data localization measures have rapidly increased in the past decade making them an increasing obstacle (Figure 5).

Annex IV. Box 1. Figure 1. Data Localization Measures



Source: López González, Casalini, and Porras (2022), "A Preliminary Mapping of Data Localisation Measures" *OECD Trade Policy Papers* No. 262, https://doi.org/10.1787/c5ca3fed-en.Note: Data localization measures are defined as explicit requirements that data be stored or processed domestically.

Annex IV. Box 2. G20 Roadmap for Enhancing Cross-Border Payments

International consensus on several priority actions (FSB 2023) could be helpful for CBDC data use and privacy protection in future.

- **Priority Action 6: Updating the application of AML/CFT rules.** FATF Recommendation 16, which applies to CBDCs, is being updated to improve the consistency, effectiveness, and efficiency of messaging in cross-border payments and facilitating more efficient AML/CFT checks. The proposed new rules were released for public consultation in February 2024[65] and discussions will be ongoing following a Private Sector Consultation planned for 2025.
- **Priority Action 7: Enhancing the interaction between data frameworks and cross-border payments.** The FSB will develop recommendations for promoting alignment and interoperability across data frameworks applicable to cross-border payments which includes data privacy.
- **Priority Action 10: Exploring enhanced use of the Legal Entity Identifier (LEI)[66] in cross-border payments.** LEI adoption is supported by the FSB and is recognized as potentially useful in strengthening data standardization as well as in assisting and supporting customer due diligence processes and sanctions screening.
- **Priority Action 14: Technical assistance (TA).** IMF and World Bank TA, which includes CBDC bilateral and regional missions, can assist in helping to align and harmonize data frameworks in line with the recommendations that will be agreed by the international community. TA will be ongoing (Murphy and others 2023).

Technology can assist in safeguarding privacy while allowing cross-border CBDC data flows. Solutions can be found when interlinking CBDCs through use of PETs. As an example, Adrian and others (2022) explore how technology can deal with data while retaining privacy and complying with regulations in a multi-currency cross-border payments and contracting platform. The platform would include information management features which can read sanctions lists and attach cryptographic proof that individuals in a transaction have been vetted. Identification and vetting services providing this information would require additional governance to ensure the information behind these proofs is reliable and trustworthy.

[62] Enhancing FATF rules on wire transfers as part of the Recommendation 16 review is included under Priority Action 6a of the revised G20 Roadmap for Enhancing Cross-Border Payments.

[63] CRS (2023). The Congressional Research Service (CRS) report “Digital Trade and Data Policy: Select Key Issues” discusses the evolution of rules governing digital trade and highlights the challenges posed by data localization requirements to digital commerce. https://crsreports.congress.gov/product/pdf/IF/IF12347/2

[64] Sai Rakshith Potluri, V Sridhar, and Shrisha Rao (2020) examine the effects of data localization on digital trade through an agent-based modeling approach, providing insights into how varying compliance costs impact digital trade dynamics.

[65] See Public Consultation on Recommendation 16 on Payment Transparency (fatf-gafi.org).

[66] The LEI is a 20-digit alphanumeric code based on the ISO 17442 standard. It uniquely identifies legally distinct entities including governmental organizations, supranationals, and individuals acting in a business capacity but excludes natural persons.

Annex V. Three Steps to Protect Privacy through privacy-by-design and Technologies

This annex provides a step-by-step approach to consider privacy protection in CBDC design. Three examples are presented to explain how to implement these steps, notably with privacy-by-design and PETs.

CBDC provides opportunities to deploy design and PETs to protect privacy. CBDC can help separate data lifecycle into segregated engineering modules, which can be protected by PETs. As PETs are relatively recent, and include very different technologies, they are still mostly confined to an academic realm, with funding from, and in cooperation with, US Federal defense and security agencies,[67] BigTech firms, and cryptocurrency foundations. As other industries are getting more familiar with the potential of PETs, they are also requesting more integration of PETs from service providers into their products.[68]

For CBDC, a clear understanding from central banks of where PETs would fit into their policy and use case objectives is needed to foster productive conversations with academic researchers and industry experts. The manner in which the central bank prioritizes various trade-offs will inform experts, similar to the way that client-facing teams at private firms communicate their requirements for adopting PETs to their research teams.

To fully reap benefits from PETs, careful design would therefore need to balance different engineering modules and technologies. Embedding privacy at an early stage of CBDC design can hence better protect privacy. Privacy protection through privacy-by-design and PETs may involve three steps:

- **Define data use cases**. These data use cases derive from the policy goals. Different data use cases might introduce conflicting requirements and trade-offs. For instance, data-driven businesses could require more data than what is needed for regulatory purposes, such as AML/CFT compliance.
- **Identify risks to privacy**. For each use case, policymakers should identify relevant risks to privacy posed by the generation, collection, and use of CBDC data. These risks should sometimes be defined by a wider public. For instance, an individual might not agree to the central bank's accessing transaction data, but this individual could agree to commercial entities accessing these transaction data. Similarly, an individual might not want the central bank to access granular transaction data, but might agree to the central bank's access to aggregated data. Examples of such a risk assessment process includes the Information Commissioner's response to the Bank of England and the UK Treasury's consultation on CBDC in the UK, and the European Data Protection Supervisor's paper on CBDCs in the EU.

[67] In the US, such agencies are NIST, MITRE, and DARPA.

[68] One example is IBM research looking into fully homomorphic encryption (FHE) to let its cloud clients save only encrypted data on the Cloud, with IBM still being able to provide blind computations on top of them. Another example is JP Morgan's secondary market customers requesting JP Morgan to build a privacy-preserving exchange, so that JP Morgan performs matching blindly without seeing its clients' books. This is described in "Privacy-preserving portfolio pricing," Proceedings of the Second ACM International Conference on AI in Finance and in a patent describing the new PET product ("Privacy-preserving portfolio pricing", Asharov and others 2021)

- **Implement privacy-by-design and PETs**. Based on the two sets of considerations discussed, CBDC teams could then devise the appropriate privacy-by-design strategy and leverage the appropriate set of PETs.

The following discussion illustrates these steps with three examples. These examples intend to emphasize how use cases and risks could determine designs and PETs.

Example 1: Privacy protection for the data collected and held by central banks

- **Define data use cases.** The policy goal is to allow central banks to administer the CBDC ledger while minimizing the conflicts of interest and privacy risks associated with collecting, storing, and handling large amounts of personal data. One example of such a data use case is the collection of personal data to satisfy AML/CFT preventive measures.
- **Identify privacy implications.** The perceived and actual risks to privacy posed by a CBDC arrangement would be where central banks, as administrators of the ledger, potentially become repositories of significant amounts of PII, including that which is needed to ensure regulatory compliance, including AML/CFT rules and regulations. Through different design options, the central bank can minimize its collection of personal information to minimize or reduce risks to privacy arising from the central bank holding and/or accessing PII. Privacy implications are explained as follows.
- **Implement privacy-by-design.**
    - In the one-tier model, the central bank would be the primary collector and processor of PII, which could lead to conflicts of interest within the organization and lead to mistrust on the part of some users. At the organizational level, separate departments should be created within the central bank so that the regulatory/supervisory functions are not intermingled with data processing functions. A second measure is for the central bank to see or access only pseudonymous identities, with PII being anonymized or sanitized where it will be handled or otherwise accessed by the central bank. With such safeguards, the central bank would not be able to access individual identity information unless pursuant to specific exemptions laid out in law.
    - In the two-tier model, the central bank will likely not directly handle PII, including as a part of AML/CFT compliance. To ensure that privacy is protected, PSPs collecting and handling PII should have rigorous data protection policies and safeguards in place. One such mechanism could be to separate the customer-facing role from the compliance function, which has been a longstanding standard practice among financial institutions with respect to traditional financial services and products. Some PII collected may be visible on the ledger without additional privacy design features to shield such data from unauthorized use and access.
    - In both models, a very carefully balanced approach that follows a thorough assessment of potential money laundering and terrorism financing risks is necessary.
    - PETs such as verified credentials, zero knowledge proofs, and blind signatures can also be used as an additional layer of protection and of separation of data to guard against unauthorized or improper access to or use of data (for example, by central banks).

Example 2: Privacy protection in PSPs

- **Define data use cases.** The policy goal is to keep transaction data private from the PSPs intermediating them, in order to protect users from threats such as targeted attacks, financial profiling, or other forms of privacy invasion that could arise from the exposure of transaction data.
- **Identify risks to privacy.** The risks to privacy would be from any PSPs that would have access to transaction data (wallet providers in a one-tier example, plus FIs in a two-tier example, and potentially even the central bank itself). If individual transactions are linkable to a user's identity, then risks of financial profiling and targeted attacks become possible.
- **Implement privacy-by-design and PETs.** Privacy-by-design solutions include separating operators collecting and processing personal data from those conducting transactions or dealing with commercial operations. In addition, data collecting or processing entities can consider additional cryptographic solutions to guarantee privacy, such as confidential transactions, ZKPs, and homomorphic and multiparty computation.[69] These solutions can also be used to generate proofs and guarantee that the data was used only in the correct circumstances by the appropriate parties. These proofs can be externally audited and communicated. While these technologies can enhance privacy, they must be carefully implemented to balance other factors such as regulatory compliance, scalability, computability between different cryptographic chosen for different use cases and security.

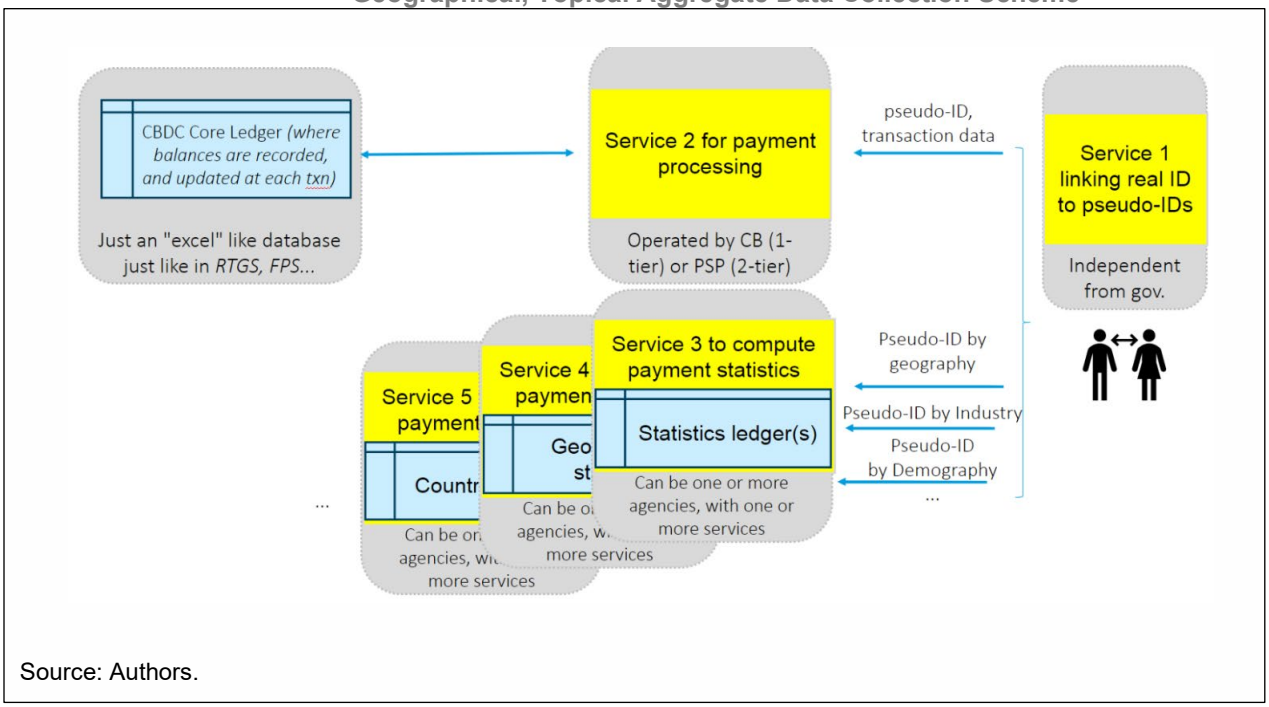
Example 3: Privacy protection by using privacy-preserving computations over masked transaction data

- **Define data use cases.** The policy goals are to allow private companies and public agencies to perform privacy-preserving computations such as the calculations of aggregate measures over an economic sector or a geography without revealing individual identities from payers and payees for macroeconomic policymaking and without creating vulnerabilities for these entities to collect more data or outside of the prescribed mandates.
- **Identify risks to privacy.** The risks to privacy could be leakage of personal data to public sector entities (such as governments and central banks) or private sector companies (such as PSPs).
- **Implement privacy-by-design and PETs.**
    - Policymakers may consider setting up trusted third parties in charge of anonymizing personal data.
    - Policymakers can consider having a trusted third party to grant multiple "pseudo-identities" labels to an individual. This third party could be the same entity as the one in charge of anonymization.

[69] Confidential Transactions is a cryptographic method where the amount involved in a transaction is encrypted. ZKPs allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement itself. Homomorphic and/or multiparty computation are forms of encryption that allows computations to be conducted on ciphertext, generating an encrypted result that, when decrypted, matches the result of operations as if they had been performed on the plaintext.

- These “pseudo-identities” labels can be geared toward different transaction engines—one transaction engine (with granular pseudo-identity) to process payments and the other transaction engines to use other pseudo-identity labels (*one transaction engine for sectorial pseudo-identity labels, one for geographical pseudo-identity label…*).
- For instance, an SME in region X and industry sector Y would receive a pseudo-identity representing region X, and another pseudo-identity representing industry sector Y. The authors illustrate this in Annex V. Figure 1. Then, each of the nonpayment processing transaction engines using only a dedicated pseudo-identity label can process and see in real times all payments going in and out of that sector or geography, without seeing any individual personal data.
- These transaction engines could also operate using the PETs as mentioned in use case 2, so that they can only see aggregated values of payments going in and out of that sector or geography, without seeing any personal data. These PETs can also generate at each time a proof that only the prescribed (encrypted) data and operations were performed. These proofs can be audited and communicated to the wider public to enhance trust.

Annex V. Figure 1. Schematic Diagram for Proposed Privacy Preserving Sectorial, Geographical, Topical Aggregate Data Collection Scheme



Source: Authors.

References

Acquisti, Alessandro, Laura Brandimarte, George Loewenstein. 2015. “Privacy and Human Behavior in the Age of Information.” *Science* 347 (6221): 509–14.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. “The Economics of Privacy.” *Journal of Economic Literature* 54 (2): 442–92.

Adrian, Tobias, Frederico Grinberg, Tommaso Mancini-Griffoli, Robert M. Townsend, and Nicolas Zhang. 2022. “A Multi-Currency Exchange and Contracting Platform.” IMF Working Paper 22/217, International Monetary Fund, Washington, DC.

Adrian, Tobias, Rodney Garratt, Dong He, and Tommaso Mancini-Griffoli. 2023. “Trust Bridges and Money Flows: A Digital Marketplace to Improve Cross-Border Payments.” IMF Fintech Notes 23/01, International Monetary Fund, Washington, DC.

Agur, Itai, Anil Ari, and Giovanni Dell’Ariccia. 2023. “Bank Competition and Household Privacy in a Digital Payment Monopoly.” International Monetary Fund, IMF Working Paper No. 2023/121.

Alshammari, Alanoud, Reem Alshammari, Maha Altalak, Khulud Alshammari and A’aeshah Alhakamy, 2022. “Credit-card Fraud Detection System using Big Data Analytics.” International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 16–18 November 2022, Maldives.

Asharov, Gilad, Tucker Balch, and Antigoni Polychroniadou. 2021. “Privacy-preserving Portfolio Pricing.” ICAIF’21: Proceedings of the Second ACM International Conference on AI in Finance, 35, pp. 1–8.

Auer, Raphael, and Boehme, Rainer. 2021. “Central bank digital currency: the quest for minimally invasive technology.” BIS Working Paper 948, Bank for International Settlements, Basel.

Auer, Raphael, Jon Frost, Leonardo Gambacorta, Cyril Monnet, Tara Rice, and Hyun Song Shin. 2021. “Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier.” BIS Working Paper 976, Bank for International Settlements, Basel.

Athey, S., Catalini, C., and Tucker, C. 2017. “The Digital Privacy Paradox: Small Money, Small Costs, Small Talk.” WP 23488, National Bureau of Economic Research, Cambridge MA.

Bharath, A., A. Paduraru, and T. Gaidosch. 2024. “Cyber Resilience of the CBDC Ecosystem.” IMF Fintech Notes 2024/003, International Monetary Fund, Washington, DC.

Chen, Long, Patrick Bolton, Bengt Holmström, Eric Maskin, Christopher Pissarides, Michael Spence, Tao Sun, Tianshu Sun, Weie Xiong, Liyan Yang, Yadong Huang, Yong Li, Xuan Luo, Yingju Ma, Shumiao Ouyang, and Feng Zhu. 2021. “Understanding Big Data: Data Calculus in the Digital Era.” Luohan Academy.

Committee on Payments and Market Infrastructures, and World Bank. 2020. “Payment Aspects of Financial Inclusion in the Fintech Era.” CPMI Papers 191, Basel, Switzerland.

Committee on Payments and Market Infrastructures and BIS Innovation Hub (BIS), International Monetary Fund (IMF), and World Bank. 2022. “Options for access to and interoperability of CBDCs for cross-border payments.” Report to the G20, Bank for International Settlements, Basel, Switzerland.

European Central Bank (ECB), 2022, “Study on New Digital Payment Methods – Executive summary.” Kantar Public Study on New Digital Payment Methods - Executive Summary (europa.eu)

FedPayments Improvements, Payments Fraud Insights, 2019. “Detecting Synthetic Identity Fraud in the US Payment System”. Federal Reserve Banks.

Financial Action Task Force. 2016. “Guidance for a Risk-Based Approach for Money or Value Transfer Services.” Paris, France.

Financial Stability Board. 2023. “G20 Roadmap for Enhancing Cross-border Payments: Consolidated Progress Report for 2023.” Basel, Switzerland.

Fleder, Michael, and Devavrat Shah. 2020. “I Know What You Bought At Chipotle for $9.81 by Solving A Linear Inverse Problem.” Proceedings of the ACM on Measurement and Analysis of Computing Systems, Volume 4, Issue 3, Article No.: 47 pp. 1–17.

G7. 2021. “Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs).” HM Treasury, London.

Goldfarb, Avi, and Catherine Tucker. 2012a. “Shifts in Privacy Concerns.” *American Economic Review* 102 (3): 349–53.

Goldfarb, Avi, and Catherine Tucker. 2012b. “Privacy and Innovation.” In *Innovation Policy and the Economy*. Vol. 12, edited by Josh Lerner and Scott Stern. Chicago: University of Chicago Press, pp. 65-90.

Haksar, Vikram, Yan Carriere-Swallow, Emran Islam, Andrew Giddings, Kathleen Kao, Emanuel Kopp, and Gabriel Quiros-Romero. 2021. “Towards a Global Approach to Data in the Digital Age.” International Monetary Fund, No. 2021/05, Washington, DC.

He, Dong, Annamaria Kokenyne, Tommaso Mancini Griffoli, Marcello Miccoli, Thorvardur Tjoervi Olafsson, Gabriel Soderberg, and Hervé Tourpe. 2023. “Capital Flow Management Measures in the Digital Age (2): Design Choices for Central Bank Digital Currency.” IMF Fintech Notes No 2023/009, International Monetary Fund, Washington, DC.

Hoepman, J.-H. 2014. “Privacy Design Strategies.” FIP International Information Security Conference, pp. 446–59. Marrakech, Morocco.

Jones, Charles I., and Christopher Tonetti. 2020. “Nonrivalry and the Economics of Data.” *American Economic Review* 110 (9): 2819–58.

Kahn, Charles M., James McAndrews, and William Roberds. 2005. “Money Is Privacy.” *International Economic Review* 46 (2): 377–99.

Kelley, Patrick Gage, Cesca, Lucian, Bresee, Joanna and Cranor, Lorrie. 2010. “Standardizing privacy notices: an online study of the nutrition label approach.” Carnegie Mellon University, Pittsburgh PA.

Koonprasert, Tayo Tunyathon, Shiho Kanada, Natsuki Tsuda, and Edona Reshidi. 2024. “CBDC Adoption: Inclusive Strategies for Intermediaries and Users.” IMF Fintech Notes, No 2024/005, International Monetary Fund, Washington, DC.

Lannquist, A., and B. Tan. 2023. “Central Bank Digital Currency’s Role in Promoting Financial Inclusion.” IMF Fintech Notes No 2023/011, International Monetary Fund, Washington, DC.

Murphy, K., T. Sun, A. Lannquist, C. Claver, K. Kao, C. Cartouni, M. Bechara, M. T. Chimienti, and O. P. Ardic Alper. 2023. “IMF and World Bank Approach to Cross-border Payments Technical Assistance.” International Monetary Fund and World Bank, Washington, DC.

OECD. 2015. “Data-driven Innovation for Growth and Well-being.” Paris.

Orestes, V., T. Silva, and H. Zhang. 2023. “Payments and Liquidity: Evidence from Extreme Weather Events in Brazil.” Draft Forthcoming.

People’s Bank of China. 2021. “Progress of Research & Development of E-CNY in China.” Report prepared by the Working Group on E-CNY Research and Development, the People’s Bank of China.

Potluri, Sai Rakshith; V. Sridhar; and Shrisha Rao. 2020. "Effects of data localization on digital trade: An agent-based modeling approach." *Telecommunications Policy*44(9).

Rubinstein, I., and N. Good. 2013. “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents.” *Berkley Technology Law Journal* 28 (2) pp. 1333-1414.

Sun, Tao, and Ryan Rizaldy. 2023. “Some Lessons from Asian E-Money Schemes for the Adoption of Central Bank Digital Currency.” Working Paper No 23/123, International Monetary Fund, Washington, DC.

Tang, MingJian, B. Sumudu U. Mendis, D. Wayne Murray, Yingsong Hu, and Alison Sutinen. 2011. “Unsupervised Fraud Detection in Medicare Australia.” Proceedings of the 9th Australasian Data Mining Conference. Ballarat, Australia.

Tucker, Catherine. 2023. “The Economics of Privacy: An agenda.” National Bureau of Economic Research, Cambridge MA.

PUBLICATIONS

Central Bank Digital Currency Data Use and Privacy Protection

NOTE/2024/004