Northwestern Journal of International Law & Business

Volume 43
Issue 3 *Spring*

Article 1

Spring 2023

Disciplining CBDCs: Achieving the Balance between Privacy Protection and Central Bank Independence

Cheng-Yun Tsang
Monash University, cheng-yun.tsang@monash.edu

Yueh-Ping Yang
National Taiwan University, yyang@sjd.law.harvard.edu

Ping-Kuei Chen
National Chengchi University, pkchen@nccu.edu.tw

 Vol. 43, No. 3
Northwestern Journal of International Law & Business

Disciplining CBDCs: Achieving the Balance between Privacy Protection and Central Bank Independence

Cheng-Yun Tsang[1], Yueh-Ping (Alex) Yang[2] and Ping-Kuei Chen[3]

Abstract

Central bank digital currency ("CBDC") is a crucial FinTech development that aspires to overhaul the current payment system. In the wake of the COVID-19 pandemic, CBDCs' promises to reduce personal contact, facilitate socially desirable use of money, and initiate more targeted monetary measures have increased their popularity. In addition, CBDCs can potentially serve as a tool to internationalize a sovereign's currency. World central banks, thus, have gradually formulated a consensus on structuring CBDCs, leaving the regulatory aspects of CBDCs deserving more attention. Among the regulatory issues related to CBDCs, observers often mentioned their association with privacy

[1] Associate Professor, Monash University Faculty of Law; Executive Group Member (Industry Partnerships), Centre for Commercial Law and Regulatory Studies (CLARS). Former Associate Professor, College of Law, National Chengchi University (NCCU), and Director of the Financial Innovation and Technological Evolution Center (FINTEC) at NCCU Law; Duke University School of Law S.J.D (2015). This paper is funded by the National Science and Technology Council of Taiwan (R.O.C) Columbus Program Young Scholars Fellowship "Constructing A Cross-Border-and-Industry Regulatory Framework for Interactions between Financial Systems and Technological Innovations" (NSTC 112-2636-H-004-001 -). The author can be reached cheng-yun.tsang@monash.edu .

[2] Associate Professor, Department of Law, National Taiwan University (NTU); Director of the Asian Center for WTO & International Health Law and Policy (ACWH) at NTU Law. Harvard Law School S.J.D. (2017). The author can be reached at alexypyang@ntu.edu.tw. Alex is the corresponding author of this paper.

[3] Associate Professor, Department of Diplomacy, National Chengchi University (NCCU); researcher at Financial Innovation and Technological Evolution Center (FINTEC) at NCCU Law. The author can be reached at pkchen@nccu.edu.tw.

This paper is a featured research and one of the four winning papers in the 6th Annual DC FinTech Week 2022 hosted by Georgetown University Law's Institute of International Economic Law in Washington DC on October 11 and 12, 2022. The authors appreciate the comments and feedback by Hilary Allen, Ross Buckley, Kimberly Houser, Colleen Baker, Virginia Harper Ho, Chien-Liang Lee, Yu-Hsin Lin, and Pasha Hsieh to this paper. The authors also appreciate the research assistance provided by Victor Wen-Yu Liao, Chin-Yun Peng, Jhen-Teng Hong, and Hsiang-Ling Kung and gratefully acknowledge the proofreading support by Georgia Fink-Brigg and the Australian Research Council Laureate Fellowship FL200100007 led by Ross Buckley.

concerns, but comprehensive studies on this aspect of CBDCs remain limited.

In this paper, we discuss the privacy concerns associated with CBDCs and attempt to introduce discipline upon CBDCs and their issuing central banks. We first demonstrate the privacy implications of CBDCs and highlight the risks that issuing sovereigns misuse CBDCs to serve their agendas. We then discuss, in a domestic context, several architectural designs proclaimed to address CBDCs' privacy concerns and propose further disciplinary mechanisms that may credibly enforce privacy protection laws against issuing central banks and other governmental authorities. We finally highlight the extraterritorial character of modern privacy laws, which allows foreign privacy protection regulators to discipline the CBDCs of other sovereigns. Through this analysis, we argue that applying modern privacy laws with proper supporting mechanisms may effectively discipline CBDCs and their issuing central banks.

Keywords: *CBDC, privacy protection, data protection, central bank independence, privacy law, programmable money, Brussels Effect*

Table of Contents

I. INTRODUCTION

CBDC is "a form of digital money or monetary value, denominated in the national unit of account, that is a direct liability of the central bank."[4] Central banks worldwide have started to devote resources to studying and developing their central bank digital currency, or CBDC.[5] As of 2022, three sovereigns have reportedly launched nationwide CBDCs, including the Bahamas's Sand Dollar, launched in October 2020, Nigeria's eNaira, launched in October 2021, and Jamaica's JAM-DEX, launched in June 2022.[6] Besides, most major economies are taking steps to experiment with their pilot CBDCs. Among them, China is perhaps the leading one, which has accumulated 360 million pilot transactions amounting to RMB 100.05 billion (equivalent to USD 14.74 billion) as of August 2022.[7] In addition to China, India launched its CBDC pilot in wholesale and retail segments in November and December 2022.[8] Russia has started the pilot program for the wholesale digital ruble in 2022 and reportedly plans to launch retail CBDC pilots in April 2023.[9] The European Union has also begun to contemplate the digital euros since 2021 and expects to conclude the investigation by the autumn of 2023.[10]

Compared to the above, the United States' progress is relatively conservative. While the Federal Reserve has started to consider the

---

[4] Ensuring Responsible Development of Digital Assets, 87 Fed. Reg. 14143, 14151 (Mar. 9, 2022) [hereinafter 2022 Executive Order]. *See also* BANK OF CAN. ET AL., CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES 3 (2020).

[5] For an interactive and dashboard-like track that shows worldwide CBDC status, *see* CBDC TRACKER, https://cbdctracker.org/ (last accessed Feb. 13, 2022, 6:56 p.m.); For a comprehensive survey, *see generally* COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES (2018), https://www.bis.org/cpmi/publ/d174.htm [hereinafter CPMI]; RYAN TODD & MIKE ROGERS, A GLOBAL LOOK AT CENTRAL BANK DIGITAL CURRENCIES: FROM ITERATION TO IMPLEMENTATION (2020).

[6] Outlook Money, *Here's All You Need to Know About Global CBDC Pilot Projects*, OUTLOOKINDIA (Dec. 23, 2022,), https://www.outlookindia.com/business/here-s-all-you-need-to-know-about-global-cbdc-pilot-projects-news-247588.

[7] 央行数字货币研究所 [People's Bank of China's Institute for Digital Currency], 扎实开展数字人民币研发试点工作 [Solidly Developing the Research and Development of the Pilot Works for Digital RMBs] (Oct. 12, 2022), http://www.pbc.gov.cn/redianzhuanti/118742/4657542/4678070/index.html.

[8] Press Release, India's Ministry of Finance, Central Bank Digital Currency (CBDC) Pilot Launched by RBI in Retail Segment has Components Based on Blockchain Technology (Dec. 12, 2022, 6:49 p.m.), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883#:~:text=The%20Minister%20stated%20in%20response,the%20paper%20currency%20and%20coins.

[9] Russia Accelerates Digital Ruble Work, Confirms It's a Way Around SWIFT, LEDGER INSIGHTS (July 27, 2022), https://www.ledgerinsights.com/russia-digital-ruble-2023-cbdc-swift/.

[10] Press Release, Eurogroup, Eurogroup Statement on the Digital Euro Project (Jan. 16, 2023), https://www.consilium.europa.eu/en/press/press-releases/2023/01/16/eurogroup-statement-on-the-digital-euro-project-16-january-2023/.

potential of creating digital dollars and facilitated the related policy discussion,[11] it has not officially decided whether to launch a U.S. CBDC.[12] The Treasury also takes a similar stance. While it acknowledges the potential benefits of digital dollars, it highlights that "further research and development on the technology that would support a U.S. CBDC is needed, *and could take years* [emphasis added]."[13] That said, the Federal Reserve has also launched some pilot programs. A notable example is the collaboration between the Federal Reserve Bank of New York and nine major banks on a proof-of-concept project on wholesale CBDC since November 2022.[14]

The motives for a central bank to issue CBDC include many facets, ranging from saving money-printing costs, combatting counterfeit money, ensuring citizens' access to the payment system, transparentizing the money flow, and facilitating the clearing and settlement of payments.[15] The adoption of CBDC further enables technology transfer and building basic infrastructure, which may facilitate technology leapfrog in a country. The Federal Reserve, for instance, acknowledged that CBDCs have the potential to provide a safe foundation for private-sector innovations to meet their demands for payment services, level the playing field in payment innovation for private-sector firms of all sizes, and generate new capabilities to meet the evolving speed and efficiency requirements of the digital economy.[16]

After the outbreak of the COVID-19 pandemic, CBDCs have received even more attention. For instance, CBDCs may facilitate remote transactions and thus help reduce personal contact and the spread of the

---

[11] *See generally* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, MONEY AND PAYMENTS: THE U.S. DOLLAR IN THE AGE OF DIGITAL TRANSFORMATION (2022) [hereinafter FEDERAL RESERVE 2022 REPORT].

[12] *Central Bank Digital Currency (CBDC) Frequently Asked Questions*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, https://www.federalreserve.gov/cbdc-faqs.htm (last visited Jan. 29, 2023).

[13] U.S. DEP'T OF THE TREAS., THE FUTURE OF MONEY AND PAYMENTS: REPORT PURSUANT TO SECTION 4(B) OF EXECUTIVE ORDER 14067 45 (2022) [hereinafter TREASURY 2022 REPORT].

[14] Press Release, Federal Reserve Bank of New York, New York Innovation Center to Explore Feasibility of Theoretical Payments System Designed to Facilitate and Settle Digital Asset Transactions (Nov. 15, 2022), https://www.newyorkfed.org/newsevents/news/financial-services-and-infrastructure/2022/20221115.

[15] *See, e.g.,* Wouter Bossu et al., *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations* (IMF Working Paper, No. W/P/20/254, 2020); Walter Engert & Ben Siu-Cheong Fung, *Central Bank Digital Currency: Motivations and Implications* (Bank of Can. Staff Discussion Paper, No. 2017-16, 2017); D. Priyadarshini & Sabyasachi Kar, *Central Bank Digital Currency (CBDC): Critical Issues and the Indian Perspective* (Institute of Econ. Growth Working Paper, No. 444, 2021). CBDC would also affect seigniorage income depending on the design. *See* CPMI, *supra* note 5, at 26.

[16] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 14-15.

virus. CBDC-based transactions may also lower the need for bank services or ATMs. They help people keep accessing banking services while banks close branch offices during the pandemic.[17] CBDCs may further enable a more targeted implementation of the bailout and monetary policies and thus help stimulate the economy slowed by the pandemic.[18]

CBDCs' impact at the international level is also significant. They may facilitate cross-border transactions by speedy and secure clearing. They may further help internationalize a sovereign's currency. Therefore, even in the United States, whose U.S. dollar possesses a dominant international role, the Federal Reserve and Treasury acknowledged the need to study the digital dollars after considering that the technological efficiency and convenience of foreign CBDCs might decrease the global use of U.S. dollars in the long run.[19]

CBDCs further lay down the technological foundation for multiple sovereigns to integrate their CBDCs into multi-CBDC arrangements to foster cross-border payment efficiency between them.[20] For instance, the Bank for International Settlements' Innovation Hub pays particular attention to the cross-border payment function of CBDCs. It has initiated numerous prominent cross-border CBDC projects to experiment with the viability of multi-CBDC arrangements, including the Project Inthanon-LionRock Phase 2, participated in by Hong Kong, Thailand, China, and UAE in 2021, Project mBridge, participated in by China, United Arab Emirates, Hong Kong, and Thailand in 2021, Project Jura, participated in by Switzerland and France in 2021, and Project Dunbar, participated in by Singapore, Australia, Malaysia, and South Africa in 2022.[21] Upon the publication of the paper, many other projects will surely take place or demonstrate progress.

The potential benefits and opportunities being said, CBDCs are not

---

[17] For the changes in payment behavior during the pandemic, *see generally* Tatjana Dahlhaus & Angelika Welte, *Payment Habits During COVID-19: Evidence from High-Frequency Transaction Data* (Bank of Can. Staff Working Paper, No. 2021-43, 2021). For the new "banking desserts," *see* Kimberly Kreiss, *Bank Branches and COVID-19: Where are Banks Closing Branches during the Pandemic?*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM (Dec. 17, 2021), https://doi.org/10.17016/2380-7172.3027.

[18] For discussion related to COVID-19 and CBDC, *see generally* Douglas W. Arner et al., *After Libra, Digital Yuan and COVID-19 : Central Bank Digital Currencies and the New World of Money and Payment Systems* (European Banking Institute Working Paper, No. 65/2020, 2020). For CBDC's function as a stimulate policy and its stimulation result, *see generally* John Barrdear & Michael Kumhof, *The Macroeconomics of Central Bank Issued Digital Currencies* (Bank of Eng. Working Paper, No. 605, 2016).

[19] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 15; TREASURY 2022 REPORT, *supra* note 13, at 34.

[20] *See generally* Raphael Auer et al., *Multi-CBDC Arrangements and the Future of Cross-Border Payments* (Bank for Int'l Settlements Papers, No. 115, 2021).

[21] MORTEN BECH ET AL., BANK FOR INTE'L SETTLEMENTS INNOVATION HUB, USING CBDCS ACROSS BORDERS: LESSONS FROM PRACTICAL EXPERIMENTS 4-9 (2022).

without concerns.[22] For one thing, CBDC might pose a substitution effect on bank deposits. Private banks need alternative finance to fund their operations as bank deposits decrease. Alternative finance may include central banks' finance, forcing central banks to undertake a more active role in this new financial landscape.[23] Depositors would also have a safer place to flee to when panic in the financial system spreads. This raises the risk and speed of commercial bank runs, which aggravates the safety and stability concerns of the whole financial system. Furthermore, depending on the technological design, CBDCs could undergo operational disruptions or cybersecurity incidents, which causes resilience concerns.[24] Last but not least, without proper design, CBDCs could be used by criminals for purposes of money laundering or financing terrorism, which raises crime prevention concerns.[25]

Among the regulatory concerns associated with CBDCs, the privacy concern stands out.[26] In a nutshell, through a CBDC's ledger, the issuing central banks may record, observe, monitor, and even control the cash flow of their currency more efficiently. This enhanced efficiency, however, inevitably implicates the privacy of general citizens, which could trigger societal unease.[27] Therefore, in the United States, the Federal Reserve listed

---

[22] For a summary, *see* FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 17-20.

[23] *See* John Crawford et al., *FedAccounts: Digital Dollars*, 89 GEO. WASH. L. REV. 113, 149-50 (2021) (noting that central banks would use discount window credits to finance private banks, eventually making private banks "appear as instrumentalities or franchisees of the state rather than as private 'intermediaries'").

[24] For instance, in its digital yuan pilot program, China reported the finding of counterfeit CBDC wallets in the market. Jane Li, *There are Already Counterfeit Wallets of China's Digital Yuan*, QUARTZ (Oct. 26, 2020), https://qz.com/1922648/there-are-already-counterfeit-wallets-of-chinas-digital-yuan.

[25] For instance, China has found cases where fraudsters used the piloting digital yuan for money laundering. *China Catches Fraudsters Using Central Bank Digital Currency for Money Laundering*, LEDGER INSIGHTS (Nov. 15, 2021), https://www.ledgerinsights.com/china-catches-fraudsters-central-bank-digital-currency-cbdc-for-money-laundering/. The G-7 has also raised the concern that China's digital yuan might be used for circumventing Western sanctions. Kosuke Takami, *China's Bid for Digital-Yuan Sphere Raises Red flags at G-7*, NIKKEI ASIA (June 5, 2021), https://asia.nikkei.com/Spotlight/Cryptocurrencies/China-s-bid-for-digital-yuan-sphere-raises-red-flags-at-G-7.

[26] For the comments raising the privacy concerns associated with CBDCs, *see, e.g.,* Aiden Slavin & Sandra Waliczek, *Privacy Concerns Loom Large as Governments Respond to Crypto*, WORLD ECON. FORUM (Apr. 14, 2022), https://www.weforum.org/agenda/2022/04/privacy-concerns-loom-large-as-governments-respond-to-crypto; Jack Schickler, *Europe's CBDC Designers Wrestle With Privacy Issues*, COINDESK (Apr. 5, 2022), https://www.coindesk.com/policy/2022/04/04/europes-cbdc-designers-wrestle-with-privacy-issues. For more optimistic view, *see* Philip Middleton, *How Real is the CBDC Threat to Privacy?*, OFFICIAL MONETARY AND FIN. INSTITUTIONS FORUM (Apr. 29, 2022), https://www.omfif.org/2022/04/how-real-is-the-cbdc-threat-to-privacy.

[27] According to a public consultation study done by the European Central Bank, 43% of the public respondents respond that privacy is the most crucial feature that they ask for a digital euro, which ranks the first among nine features under the survey. EUROPEAN CENTRAL

"privacy-protected" as the first of the four core qualities of a digital dollar.[28] In Europe, the Eurogroup stressed that for the digital euro to succeed, it must ensure and maintain users' trust, "for which privacy is a key dimension and a fundamental right."[29] The G-7 also expressed their concern that China's digital yuan might allow the Chinese government access to transaction data and use it to infringe data privacy, suppress speech, and push out political opponents.[30]

In theory, issuing central Banks may address CBDCs' privacy concerns by keeping anonymity with their CBDC design. Nevertheless, many contradicting considerations preclude central banks from issuing anonymous CBDCs. Specifically, many CBDCs' benefits are available only if central banks collect and process user data, such as transparentizing the money flow to facilitate anti-money laundering and counter-terrorist financing (AML/CFT) measures or carrying out more targeted monetary actions.

In the United States, the Federal Reserve has expressly negated the idea of an anonymous CBDC, stressing that a digital dollar, if any, must be identity-verified to combat money laundering and the financing of terrorism.[31] In Europe, which emphasizes that CBDC's design must ensure a high level of privacy, the Eurogroup composed of ministers from the Euro area also acknowledges the need to harmonize the privacy concern with "other policy objectives such as preventing money laundering, illicit financing, tax evasion, and ensuring sanctions compliance."[32] Similarly, in China, the People's Bank of China has made it clear that "[a] completely anonymous CBDC is not feasible"[33] and adopts the so-called "managed anonymity" approach.[34]

If CBDCs are not anonymous, their privacy concerns would inevitably

---

BANK, EUROSYSTEM REPORT ON THE PUBLIC CONSULTATION ON A DIGITAL EURO 10-11 (2021).

[28] Craig Torres, *Powell Says Digital Dollar Must Ensure Privacy, Identification*, BLOOMBERG (Mar. 23, 2022), https://www.bloomberg.com/news/articles/2022-03-23/powell-says-digital-dollar-must-ensure-privacy-identification?leadSource=uverify%20wall; *See also* FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 13-14.

[29] Press Release, Eurogroup, Eurogroup Statement on the Digital Euro Project (Jan. 16, 2023), https://www.consilium.europa.eu/en/press/press-releases/2023/01/16/eurogroup-statement-on-the-digital-euro-project-16-january-2023.

[30] Takami, *supra* note 25. *See also* Roula Khalaf & Helen Warrell, *UK Spy Chief Raises Fears over China's Digital Renminbi*, FINANCIAL TIMES (Dec. 11, 2021), https://www.ft.com/content/128d7139-15d6-4f4d-a247-fc9228a53ebd (identifying that CBDC gives "a hostile state the ability to surveil transactions" and "exercise control over what is conducted on those digital currencies").

[31] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 13-14.

[32] Eurogroup, *supra* note 29.

[33] Changchun Mu, *Balancing Privacy and Security: Theory and Practice of the E-CNY's Managed Anonymity*, at 5 (2022), http://www.pbc.gov.cn/en/3688006/4706656/4696666/2022110110364344083.pdf.

[34] *See generally id.*

manifest. Balancing the utility of CBDCs against their privacy concerns thus becomes a challenge for CBDCs' ongoing development. Currently, an increasing number of central banks, international organizations, and academic studies have noticed the importance of this challenge and proposed solutions. Some proposals rely on technological designs to address it, such as adopting the so-called "token-based CBDCs."[35] Some proposals rely on architectural designs to control the privacy concerns, such as adopting the so-called "intermediated CBDCs."[36] Some studies believe that the existing privacy regulations have adequately addressed CBDCs' privacy concerns, under which central banks and other related parties simply need to comply with their privacy protection obligations.[37] In general, the current studies appear optimistic that CBDCs' privacy concerns are controllable.[38]

In this paper, we reflect on the existing proposals and illustrate how they have underestimated the complexity of this issue. In a nutshell, privacy protections are easier said than done. There is an inherent informational asymmetry between CBDC users and the potential CBDC data controllers, including the central bank, its partnering intermediaries, and other government authorities. In the eyes of CBDC users, it is unclear which entities control what type of CBDC data. It is also unclear whether the entities controlling their CBDC data follow the privacy protection requirements. This information asymmetry is the root cause of the public perception that CBDCs may ultimately lead to a surveillance state. To address this inherent distrust, a central bank's mere statement that it has adopted adequate technological designs, architectural designs, or privacy

---

[35] *See, e.g.,* Karin Thrasher, *The Privacy Cost of Currency*, 42 MICH. J. INT'L L. 403 (2021). In a similar vein, the European Central Bank attempts to explore whether a DLT-based solution may preserve CBDCs' anonymity and tends to permit anonymous CBDCs in low-value and low-risk payments. *See generally* EUROPEAN CENTRAL BANK, EXPLORING ANONYMITY IN CENTRAL BANK DIGITAL CURRENCIES (2019). *See also Lagarde: 'Low-Value, Low-Risk' Digital Euro Payments Could Be Anonymous*, PYMNTS (Nov. 14, 2022), https://www.pymnts.com/cbdc/2022/lagarde-low-value-low-risk-digital-euro-payments-could-be-anonymous/#:~:text=As%20such%2C%20Lagarde%20said%20the,public%20interest%20in%20preventing%20illicit.

[36] *See, e.g.,* HOWELL JACKSON & TIMOTHY MASSAD, THE BROOKINGS INSTITUTION, THE TREASURY OPTION: HOW THE US CAN ACHIEVE THE FINANCIAL INCLUSION BENEFITS OF A CBDC NOW 15-16 (2022). For an introduction of the intermediated CBDC, *see* Raphael Auer & Rainer Böhme, Bank for Int'l Settlements, *Central Bank Digital Currency: The Quest for Minimally Invasive Technology* 9-14 (Bank for Int'l Settlements Working Paper, No. 948, 2021); BANK FOR INT'L SETTLEMENTS, ANNUAL ECONOMIC REPORT 77-80 (2021) [hereinafter BIS 2021 ANNUAL REPORT]. The United States appears to favor this approach. *See* FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 13-14; TREASURY 2022 REPORT, *supra* note 13, at 36-37.

[37] *See, e.g.,* Crawford et al., *supra* note 23, at 164-67.

[38] China, for instance, appears confident that digital yuan's managed anonymity is sufficient to balance the privacy concerns and other policy objectives. Mu, *supra* note 33, at 2-5.

protection compliance is not enough.[39] Disciplines are needed not only in operational terms but also in institutional terms. Not only should the CBDC's operations be disciplined, but also should the central bank's.

However, disciplining CBDCs and the central bank for privacy reasons might introduce external supervisors into CBDC's regulatory landscape. To begin with, disciplining the privacy protection measures of central banks involves imposing privacy protection requirements on central banks. However, as mentioned above, even if related disciplinary mechanisms are already in place, ensuring the credibility of these mechanisms remains challenging. This challenge begs a separate set of legal designs. For instance, a robust check-and-balance mechanism against central banks is warranted to enforce the legal requirements under privacy protection laws credibly. Therefore, a data protection authority separate from the central bank shall be present. In that case, which agency should be charged with enforcing disciplinary action against central banks? With what kind of regulatory tools? These regulatory issues call for a sophisticated set of legal and institutional designs.

On the other hand, introducing separate privacy supervisors for central banks might put central bank independence at risk. After all, the CBDC data controlled by central banks and other partnering intermediaries is extremely valuable. Other governmental authorities and politicians would be keen to obtain the CBDC data for policy purposes, such as crime prevention and detection, or political purposes, such as elections. Introducing a credible disciplinary mechanism against central banks creates a space for other governmental authorities or politicians to intervene in the central bank's operation. Therefore, the legal and institutional designs for CBDCs shall not only balance between privacy concerns and other policy objectives, such as AML/CFT. They shall further consider the potential abuse that could compromise central bank independence. Essentially, they shall balance between three main pillars: privacy protection, the pursuit of other policy objectives, and central bank independence.

Striking the above balance is even more complicated in an international setting. As mentioned, CBDCs have the potential to evolve into more efficient cross-border payment instruments that help internationalize a sovereign's currency. This means that the citizens of other receiving sovereigns may hold a sovereign's CBDC. To that extent, the issuing central bank may control the receiving sovereign's citizen data and thus trigger privacy concerns in receiving sovereigns.

To control these concerns, receiving sovereigns might exert the so-called "Brussels Effect" of modern privacy laws,[40] that is, applying their

[39] This somehow explains why, as mentioned above in Footnote 30, the international community expressed their distrust of China's digital yuan notwithstanding the digital yuan's managed anonymity design.

[40] The term "Brussels Effect" is a term first used by Anu Bradford in 2012 to describe

privacy laws extraterritorially to the issuing central bank, the related government authorities, or the partnering intermediaries. For instance, the Treasury of the United States has made it clear that "the United States has an interest in ensuring that such systems are aligned with the principles of privacy, human rights, and other democratic values."[41] Therefore, when a sovereign's CBDC goes international, it might be subject to not only domestic privacy laws but also multiple foreign ones.

We argue that the above Brussels Effect aspect of CBDC is a double-edged sword. On the one hand, foreign privacy laws and supervisors could be more independent and thus credible, considering that the issuing central bank has less opportunity to compromise or capture foreign privacy supervisors. On the other hand, a sovereign may use its privacy laws to serve the protectionism purpose. For instance, it may effectively prevent other sovereigns' CBDCs from circulating in its territory on the grounds that issuing central banks and their partnering intermediaries do not adequately protect its citizens' privacy. If most major sovereigns take advantage of the Brussels Effect of their privacy laws and game the disciplines of other sovereigns' CBDCs, it would create a silo effect on all CBDCs, which limits the cross-border circulation of each sovereign's CBDC. In that case, any CBDC would find it challenging to evolve into a cross-border payment instrument.

International coordination on privacy disciplines over CBDCs is undoubtedly warranted to break up the above tie. For instance, the Treasury of the United States has highlighted the U.S. government's active international engagement to promote CBDC technologies that meet its domestic values and legal requirements.[42] Indeed, an increasing number of bilateral, plurilateral, or multilateral agreements contain personal information protection provisions and attempt to promote compatibility between different privacy laws.[43] However, since these international coordination efforts are in the form of trade agreements, a sovereign's central bank would naturally need assistance from its trade departments or even the privacy supervisor to initiate the international coordination. To that extent, central bank independence is, again, at risk. This international perspective of CBDC thus formulates a different triangular relationship between privacy protection, cross-border payment efficiency, and central bank independence.

---

how the European Union sets global standards for the international business environment and thus wields its international influence. For a comprehensive introduction, *see generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020).

[41] TREASURY 2022 REPORT, *supra* note 13, at 36.

[42] TREASURY 2022 REPORT, *supra* note 13, at 36-37.

[43] *See, e.g.,* Comprehensive and Progressive Agreement for Trans-Pacific Partnership, art. 14.8(5), Mar. 8, 2018 [hereinafter CPTPP]; Digital Economy Partnership Agreement, art. 4.2(6), June 12, 2020 [hereinafter DEPA].

In this paper, we attempt to delve into the privacy concerns of CBDCs and discuss the associated implications from domestic and international perspectives. In Part II, we elaborate on CBDCs' privacy concerns and the challenges posed by CBDCs to central bank independence. In Part III, we discuss potential CBDC designs proclaimed to address privacy concerns and specify three disciplinary mechanisms to enforce privacy laws in a domestic context. In Part IV, we move to the international aspect of CBDCs and highlight that the Brussels Effect of modern privacy laws may introduce foreign disciplines against issuing central banks but also lead to the silo effect of CBDCs. While the privacy law harmonization initiatives for addressing the silo effect are encouraged, they could also put central bank independence at risk. We conclude this paper in Part IV. In sum, we anticipate that central banks will encounter internal and external pressure to enhance CBDCs' privacy protection during the design phase, which is likely an *orderly* development of CBDCs.

II. PRIVACY CONCERNS OF CBDCS AND THE CHALLENGES OF CENTRAL BANK INDEPENDENCE

A. A Primer of CBDCs

Despite sharing similar propensities, CBDCs differ from ordinary or private-sector-issued crypto-assets, such as Bitcoin or Ether. Crypto-assets refer to "representations of value or claims in digital form that rely on the use of a method of distributed ledger technology (DLT)" and typically exclude CBDCs from their scope.[44] Crypto-assets are not backed by or connected to a sovereign currency,[45] whereas CBDCs are highly connected to a sovereign currency.

CBDCs also differ from other private money, such as commercial bank money or other nonbank money. Commercial bank money is the digital form of money held in accounts at commercial banks. In contrast, nonbank money is the digital form of money held as balances at nonbank financial service providers (such as payment service providers ("PSPs")).[46] Although private money is typically connected to a sovereign currency by promising the conversion into public money on a one-for-one basis on demand, it represents a promise issued by the private sector. Therefore,

[44] U.S. DEP'T OF THE TREAS., CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES 4 (2022).

[45] An exception is stablecoins, which refers to "a category of cryptocurrencies with mechanisms that are aimed at maintaining a stable value, such as by pegging the value of the coin to a specific currency, asset, or pool of assets or by algorithmically controlling supply in response to changes in demand in order to stabilize value." 2022 Executive Order, *supra* note 4, § 9(e). To the extent that a stablecoin pegs its value to a specific currency, which is the majority case, it is connected to a sovereign currency.

[46] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 5.

private money is susceptible to runs.[47] By contrast, CBDCs are issued by the public sector, that is, the central bank, representing the central bank's direct liability.

Depending on its architecture, CBDCs can be further classified into the following categories:

1. Wholesale versus Retail

Depending on their application scope, CBDCs can be used at a wholesale level or retail level. Wholesale CBDCs have restricted access and are used for wholesale payment and settlement transactions. By contrast, retail CBDCs, also known as general purpose CBDCs, are widely available and primarily targeted at retail transactions and other broader uses.[48] Wholesale CBDCs are generally intended for banks and other financial institutions, while retail CBDCs are designed to be accessed and used by many consumers and businesses.[49]

Wholesale CBDCs may be designed to facilitate large-value financial transactions, such as a settlement asset for digital clearinghouses. Retail CBDCs may be intended as an alternative to the existing payment instruments such as cash, checks, credit or debit cards, etc.[50] Most central banks start their CBDC pilots from wholesale CBDCs. Recently, many central banks have shifted their focus to retail CBDCs.[51]

2. Direct versus Indirect

Central banks may design their CBDCs as direct or indirect claims to themselves. Direct CBDCs represent a direct claim of CBDC users against the central bank. Contrastly, indirect CBDCs, also known as synthetic CBDCs, refer to the liabilities issued by private PSPs matched by funds held at the central bank.[52] Some studies also term indirect CBDCs or synthetic CBDCs as "CBDC-backed e-money."[53]

Direct CBDCs resemble a central bank's digital cash and are less subject to runs. By contrast, indirect CBDCs resemble private money issued

---

[47] TREASURY 2022 REPORT, *supra* note 13, at 3-4.

[48] CPMI, *supra* note 5, at 4.

[49] TREASURY 2022 REPORT, *supra* note 13, at 19.

[50] *Id.* at 19-20.

[51] Press Release, Bank for Int'l Settlements, Central Banks and the BIS Explore What a Retail CBDC Might Look Like (Sept. 30, 2021), https://www.bis.org/press/p210930.html.

[52] BANK OF CAN. ET AL., *supra* note 4, at 4. For an introduction of synthetic CBDC, *see* Tobias Adrian & Tommaso Mancini-Griffoli, *The Rise of Digital Money* 14-15 (IMF Fintech Notes, No. NOTE/19/01, 2019), https://www.imf.org/-/media/Files/Publications/FTN063/2019/English/FTNEA2019001.ashx.

[53] HONG KONG MONETARY AUTHORITY (HKMA), E-HKD: A TECHNICAL PERSPECTIVE 12 (2021), https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/e-HKD_A_technical_perspective.pdf.

and operated by private PSPs.[54] To the extent that the central bank can ensure that these private operators' funds at the central bank match their liabilities, indirect CBDCs may resemble direct CBDCs.[55] However, the central bank may not have sufficient information to perform this oversight duty.[56]

3. Account-Based versus Token-Based

Central banks may design their CBDC as account-based or token-based.[57] Account-based CBDCs refer to CBDCs tied to an identification scheme such that all users need to identify themselves to access it.[58] In other words, in the case of account-based CBDCs, users must pass the verification to access and spend the CBDCs based on the CBDC user's identity. Therefore, account-based CBDCs typically lack cash-like characteristics and cannot be transferred anonymously.[59]

By contrast, token-based CBDCs refer to CBDCs secured via

---

[54] Some studies do not consider indirect CBDCs as CBDCs because their holders do not have a direct claim against the central bank. It also highlights that indirect CBDCs lack the neutrality and liquidity of central bank money. BANK OF CAN. ET AL., *supra* note 4, at 3-4, 3 n.1.

[55] BANK OF CAN. ET AL., *supra* note 4, at 4.

[56] HKMA, *supra* note 53, at 11-12.

[57] In this paper, we refer to the criterion adopted by the Bank for International Settlements ("BIS") for distinguishing between account-based and token-based CBDCs. We note that studies may adopt different criteria for distinguishing between account-based and token-based systems. For instance, some economic literature defines account-based systems as record systems that "require the keeping of accounts in the name of the payer and payee," with their success hinging, most fundamentally, on "the ability of its participants to verify the identities of account holders, to ascertain the link between transactors and histories." In contrast, they define token-based systems as store-of-value systems that "are founded on the transfer of some payments object between payer and payee, and depend critically on a payee's ability to verify the payment objects." In other words, to sufficiently verify the validity of a payment transaction, a token-based system requires verifying the validity of the object used to pay, whereas, an account-based system requires verifying the identity of the payer. Aldar C-F. Chan, *UTXO in Digital Currencies: Account-based or Token-based? Or Both?* (2021), at 3-4, https://arxiv.org/abs/2109.09294 (last visited Feb. 11, 2023). While this conceptual distinction, in general, resembles the one adopted by the BIS, it effectively envisages a narrow scope of token-based CBDCs. For instance, the so-called "unspent transaction outputs" system (the "UTXO-based system"), a system often portrayed as contrasting to the account-based system, may be classified as an account-based system according to the criteria adopted by the economic literature. In fact, under this criterion, perhaps no digital records may fall within the category of the token-based system, leaving only physical payments in the token-based system. *See generally id.* Therefore, we refer to BIS's criterion, under which the UTXO-based system may fall within the account-based or token-based system, depending on the level of anonymity adopted by the system. This is also the approach adopted by the Hong Kong Monetary Authority ("HKMA"). HKMA, *supra* note 53, at 22, 29-30.

[58] BIS 2021 ANNUAL REPORT, *supra* note 36, at 91.

[59] Arner et al., *supra* note 18, at 30.

passwords such as digital signatures that can be accessed anonymously.[60] Therefore, token-based CBDCs do not necessarily require identification checks for each CBDC user. On that account, token-based CBDCs resemble cash or Bitcoin.[61] Central banks can further design token-based CBDCs into different degrees of anonymity.[62]

4. One-Tier versus Two-Tier

Central banks may design their CBDCs as one-tier or two-tier. Under one-tier CBDCs, also known as direct CBDCs, each CBDC user has an account with direct access to the central bank.[63] In the one-tier CBDC, the central bank fully operates the CBDC system, including account opening, account maintenance, enforcement of AML/CFT rules, and day-to-day user service. It is generally agreed that one-tier CBDCs tax central banks' excessive operational burden and might negatively impact innovation.[64]

By contrast, under two-tier CBDCs, central banks delegate most operational tasks and user-facing activities to private partnering intermediaries, including commercial banks, non-bank PSPs, and others. Under this architecture, CBDC users do not have direct accounts with central banks. Instead, these private partnering intermediaries link CBDC users to central banks, handling the operational tasks such as AML or CFT for central banks.[65] Central banks can thus focus on providing core and foundational CBDC infrastructure.

There are various ways to design two-tier CBDCs. The first one is a variant of the one-tier CBDCs. Under this simplest model, central banks only delegate the user-facing and authentication tasks to private partnering intermediaries. However, users remain to have direct accounts at central banks. Central banks, thus, still maintain the retail balances and process retail transactions.[66]

The second one is "hybrid CBDCs." Under this architecture, central banks delegate private partnering intermediaries to process all retail transactions in real-time besides user-facing tasks and user authentication. That said, central banks remain to record all retail balances as communicated by the intermediaries. Therefore, although central banks do not process retail transactions, they control the retail records.[67] On the other hand, although the private partnering intermediaries handle retail

---

[60] BIS 2021 ANNUAL REPORT, *supra* note 36, at 92.

[61] Arner et al., *supra* note 18, at 30.

[62] CPMI, *supra* note 5, at 6.

[63] Arner et al., *supra* note 18, at 30.

[64] *See, e.g.,* BIS 2021 ANNUAL REPORT, *supra* note 36, at 77-79; HKMA, *supra* note 53, at 10.

[65] Arner et al., *supra* note 18, at 31-32.

[66] HKMA, *supra* note 53, at 11.

[67] *Id.*

transactions for CBDC users, these users hold claims directly against central banks instead of these intermediaries.[68]

The third one is "intermediated CBDCs." Under this architecture, central banks do not record any retail balance. Instead, they only keep wholesale balances of individual partnering intermediaries. Therefore, only the respective intermediaries withhold and maintain detailed records of retail transactions and balances.[69] To the extent that central banks do not withhold the retail records but remain obliged to honor these retail claims, they need to supervise partnering intermediaries to ensure the integrity and availability of these records.[70] The Federal Reserve of the United States appears to favor this architecture.[71]

5. Centralized versus Distributed

CBDC payment involves the transfer of central bank liability recorded on a ledger. Central banks can determine how to design the CBDC ledger.[72] A central bank may consider adopting a centralized ledger to record CBDC data. A centralized ledger, in turn, requires a central institution, typically the central bank, to administer the ledger and transfer the liabilities.[73]

In contrast, a central bank may consider adopting a distributed ledger by employing distributed ledger technology ("DLT"), such as blockchain, to record CBDC data. The DLT-based system for administering the CBDC ledger can be permissioned or permissionless.[74] For instance, the Federal Reserve of the United States is considering using DLT for wholesale payments.[75]

Besides centralized and distributed ledgers, there are other variants. For instance, a central bank may consider a centralized ledger with a small number of data centers or a centralized ledger with a cap on allowable offline transactions.[76]

---

[68] Auer & Böhme, *supra* note 36, at 11.

[69] HKMA, *supra* note 53, at 11-12.

[70] Auer & Böhme, *supra* note 36, at 12.

[71] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 13-14 (noting that "[w]hile no decisions have been made on whether to pursue a CBDC, analysis to date suggests that a potential U.S. CBDC, if one were created, would best serve the needs of the United States by being privacy-protected, intermediated, widely transferable, and identity-verified", and highlighting the merits of intermediated CDCs by stating that "[a]n intermediated model would facilitate the use of the private sector's existing privacy and identity-management frameworks; leverage the private sector's ability to innovate; and reduce the prospects for destabilizing disruptions to the well-functioning U.S. financial system").

[72] For the discussion of other ledger design choices, *see* BANK OF CAN. ET AL., *supra* note 4, at 12-13.

[73] TREASURY 2022 REPORT, *supra* note 13, at 21.

[74] *Id.*

[75] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 23.

[76] BANK OF CAN. ET AL., *supra* note 4, at 14-15.

6. Interest-bearing versus Non-interest-bearing

Central banks also need to determine whether their CBDCs bear interest or not. Interest-bearing CBDCs, or deposit-like CBDCs, may incentivize the general public to hold CBDCs instead of depositing CBDCs in the bank account. The concern, however, is that if the general public substitutes interest-bearing CBDCs for bank deposits on a large scale, commercial banks would face funding problems.[77] Moreover, this substitution effect might further compromise the financial intermediary role of banks in an economy.[78]

In contrast, non-interest-bearing CBDCs, or cash-like CBDCs, do not trigger this concern.[79] Some studies further propose a tiering interest rate system for CBDCs, under which the interest rate decreases as the volume of CBDCs held by individuals increases.[80]

7. Summary

As the understanding of CBDC increases, world central banks have gradually formulated several consensuses on CBDCs' architectural designs. For instance, they often start by experimenting with wholesale CBDCs and then consider proceeding to experiment with retail CBDCs.[81] They generally prefer direct CBDCs over indirect CBDCs because they envisage cash-equivalent CBDCs.[82] They prefer account-based CBDCs over token-based CBDCs because they need to address AML/CFT concerns, but they tend to preserve a small scale of token-based CBDCs.[83] While some sovereigns prefer to adopt interest-bearing CBDCs but set a limit on the interest rate to prevent an excessive challenge to the existing banking system,[84] more sovereigns prefer non-interest-bearing CBDCs to avoid competition with commercial banks.[85] Most central banks tend to adopt

[77] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 17.

[78] For related studies, *see* CPMI, *supra* note 5, at 14-17.

[79] *Id.*

[80] *See generally* Ulrich Bindseil, *Tiered CBDC and the Financial System* (European Central Bank Working Paper, Paper No. 2351, 2020).

[81] Taking the United States, the latecomer in CBDC, for instance. While the United States has not launched any retail CBDC pilots as of 2022, the Federal Reserve Bank of New York has started to conduct a proof-of-concept project on wholesale CBDCs with major financial institutions since November 2022. Federal Reserve Bank of New York, *supra* note 14.

[82] Raphael Auer et al., *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies* 5 (Bank for Int'l Settlements Working Paper, Paper No. 880, 2020).

[83] *Id.* at 5.

[84] *Id.* at 36.

[85] Florian Böser & Hans Gersbach, *Monetary Policy with a Central Bank Digital Currency: The Short and the Long Term* (Centre for Economic Policy Research Working Paper Series, Paper No. DP15322, 2020), https://cepr.org/publications/dp15322 ; Itai Agur et al., *Designing Central Bank Digital Currencies*, 125 J. MONETARY ECON. 62 (2022).

centralized CBDCs for the time being while acknowledging the potential of DLT-based CBDCs in the long run.[86]

Moreover, the consensus among policymakers is that CBDCs have the most advantages through a two-tier architecture.[87] While one-tier CBDCs have the advantage of reducing the intermediary process and saving the intermediary costs, two-tier CBDCs receive more popularity for several reasons. First, two-tier CBDCs bring the slightest challenge to the existing financial system. Banks and PSPs may continue servicing their CBDC users. The difference is that they are not providing deposit or payment services on their accounts but CBDC intermediary services as the issuing central banks' agents.

Second, two-tier CBDCs introduce private partnering intermediaries to assist central banks in providing user services. This public-private partnership is a more efficient allocation of duties because central banks would find it challenging to handle the day-to-day operations of a CBDC.[88] For instance, under two-tier CBDCs, central banks can delegate AML and CFT tasks to private partnering intermediaries, which saves them the costs and labor required for these legal compliance works. For another instance, two-tier CBDCs introduce private sectors that have the advantage of promoting innovation and competition and driving flexibility, convenience, and adoption.[89]

Third, one-tier CBDCs are not only subject issuing central banks to daily KYC tasks. They also put the whole banking system at risk by causing deposit outflows from commercial banks to the issuing central bank, which fundamentally undermines the contemporary financial intermediary system.

B. CBDCs: A New Mandate of Central Banks

1. The Expanding Mandates of Central Banks

Modern central banks are responsible for many mandates beyond their original design. Central banks nowadays are involved in managing monetary policies, ensuring full employment, taming inflation, stimulating the economy, promoting financial inclusion, ensuring a robust financial system, and even tackling climate changes and inequality.[90] These mandates

---

[86] Arner et al., *supra* note 18, at 45. The finding is that DLT might have the advantage in resilience and the potential to make secure peer-to-peer and offline payments. However, the existing experiments show that DLT is quite inefficient when it comes to retail CBDCs. Some central banks are also considering adopting partial DLT to build their CBDC, but this is a DLT system that is very different from the technology used in cryptocurrencies.

[87] Auer et al., *supra* note 82, app. B at 4-5.

[88] Arner et al., *supra* note 18, at 47.

[89] BANK OF CAN. ET AL., *supra* note 4, at 16.

[90] For discussions about central banks' various roles, *see* Randall S Kroszner, *Comments on Charles Goodhart's paper "The Changing Role of Central Banks": What Should Central Banks Do?* 22–23 (Bank for Int'l Settlements Working Paper, Paper No. 326, 2010),

gradually erode the independence of central banks as they play a greater role in the welfare of citizens and subject them to domestic political pressure.[91]

So far, these mandates are mostly related to achieving government objectives through macroeconomic management. Central banks adopt various policies to achieve policy objectives requested by governments. Sometimes these objectives are not in accordance with central banks' desired policies, and central bankers may resist these requests. This principal-agent problem becomes severe as central banks struggle to maintain independence.[92] A typical example of this problem is that a government would request its central bank to stimulate the economy with monetary tools, which is a politically popular decision. However, the central bank would be reluctant to follow the government's request because it is originally designed to combat inflation and maintain financial stability.

Such struggles became more frequent during the COVID-19 pandemic. The grim economic prospect under lockdown and the health emergency further pushed governments to ask their central banks to play a role in salvaging the economic downturn.[93] Central banks are forced to conduct countercyclical stimulus measures to keep the economy from failing. Sometimes central bankers may compromise their professional judgment to implement policies their governments favor. Frictions between the two have become more common. President Trump's criticism of

---

https://www.bis.org/publ/work326.pdf. *See also* Adina Criste & Iulia Lupu, *The Central Bank Policy between the Price Stability Objective and Promoting Financial Stability*, 8 PROCEDIA ECON. & FIN. 219 (2014); Philip Harvey, *What is Full Employment-and Why the Definition Matters* (2016), https://tinyurl.com/2or6mo52; Alex Cukierman et al., *Measuring the Independence of Central Banks and Its Effect on Policy Outcomes*, 6 WORLD BANK ECON. REV. 353 (1992); Sander Oosterloo & Jakob de Haan, *Central Banks and Financial Stability: A Survey*, 1 J. FIN. STABILITY 257 (2004); Simon Dikau & Ulrich Volz, *Central Bank Mandates, Sustainability Objectives and the Promotion of Green Finance*, 184 ECOLOGICAL ECON. 107022 (2021); Donato Masciandaro & Riccardo Russo, *Central Banks and Climate Policy: Unpleasant Trade–Offs? A Principal–Agent Approach* (BAFFI CAREFIN Centre Working Paper, Paper No. 181, 2022).

[91] Mervyn King & Dan Katz, *Central Banks Are Risking Their Independence*, BLOOMBERG (Aug. 23, 2021), https://www.bloomberg.com/opinion/articles/2021-08-23/central-banks-are-risking-their-independence-mervyn-king-dan-katz. *See also* Jakob de Haan et al., *Central Bank Independence Before and After the Crisis*, 60 COMPAR. ECON. STUD. 183 (2018).

[92] *See, e.g.,* Michele Fratianni et al., *Central Banking as a Political Principal-Agent Problem*, 35 ECON. INQUIRY 378 (1997); Robert Elgie, *The Politics of the European Central Bank: Principal-Agent Theory and the Democratic Deficit*, 9 J. EUR. PUB. POL'Y 186 (2002); Stanley Fischer, *Central-Bank Independence Revisited*, 85 AM. ECON. REV. 201 (1995); Massimiliano Castelli & Stefan Gerlach, *Central Banks are Too Risk Averse as Investors* (SUERF Policy Note, No. 78, 2019).

[93] For example, the US Federal Reserve stepped in and helped the country containing economic damages resulting from the pandemic. Eric Milstein & David Wessel, *What did the Fed do in response to the COVID-19 Crisis?*, BROOKINGS (Dec. 17, 2021), https://www.brookings.edu/research/fed-response-to-covid19/.

Federal Reserve policies, Turkish President Erdogan's expulsion of central bankers, and Azerbaijan President Aliyev's dismissal of his central bank governor, who served 27 years, all suggest that government intervention into central banks has become increasingly stringent.[94]

As the financial world digitalizes, the central bank has a new mandate: CBDCs. Many sovereigns have been exploring, testing, and developing CBDCs.[95] It is widely believed that the urgency to promote electronic payment and financial inclusion, and the need to respond to the rise of private sector crypto-assets gave this trend momentum.[96] The rise of global stablecoins, particularly the challenge posed by Facebook's Libra or Diem projects, also forces central banks to think seriously about digitalizing their currencies.[97]

Increased sovereigns have adopted or experimented with CBDCs. As illustrated in Part I of this paper, as of 2022, the Bahamas, Nigeria, and Jamaica have adopted retail CBDCs. Besides them, many sovereigns launched CBDC pilots to experiment with the issuance of CBDCs. Sweden was reportedly the first sovereign officially announcing their work on retail CBDCs.[98] It launched the "e-Krona" project to experiment with CBDCs in 2017[99] and entered the second phase of pilots in February 2021.[100] In addition to Sweden, China commenced its Digital Currency Electronic

---

[94] *See* Sarah Binder & Mark Spindel, *Why is Trump Attacking the Federal Reserve? We Answer Your Questions.*, WASH. POST (Aug. 27, 2019), https://www.washingtonpost.com/politics/2019/08/27/why-is-trump-attacking-federal-reserve-we-answer-your-questions; Francesco Bianchi et al., *Threats to Central Bank Independence: High-Frequency Identification with Twitter* (Nat'l Bureau of Econ. Rsch. Working Paper, No. 26308, 2019); Anna Hirtenstein & Jared Malsin, *Turkey's Erdogan Fires Central Bank Officials, Fueling Economic Uncertainty*, WALL ST. J. (Oct. 14, 2021), https://www.wsj.com/articles/turkeys-erdogan-fires-central-bank-officials-fueling-economic-uncertainty-11634209321; Dan Hardie, *Azerbaijan Appoints New Governor after Dismissing Predecessor*, CENTRAL BANKING (Apr. 13, 2022), https://www.centralbanking.com/node/7946306.

[95] For a summary, *see generally* ANNEKE KOSSE & ILARIA MATTEI, *Gaining momentum – Results of the 2021 BIS Survey on Central Bank Digital Currencies* (Bank for Int'l Settlements Paper, No. 125, 2022).

[96] Gita Bhatt, *Reimagining Money in the Age of Crypto and Central Bank Digital Currency*, IMF BLOG (Sept. 1, 2022), https://www.imf.org/en/Blogs/Articles/2022/09/01/reimagining-money-in-the-age-of-crypto-and-central-bank-digital-currency. *See also* Kelly-Ann Coulter, *'Stop Creating Private Money!': Should the Bank of England Introduce a Central Bank Digital Currency to Compete with Cryptocurrency? A Review of the UK Bank of England's Proposed Retail CBDC* (2022), https://papers.ssrn.com/abstract=4078059 (last visited Oct 15, 2022); Sally Chen et al., *CBDCs in Emerging Market Economies* (Bank for Int'l Settlements Paper, No. 123, 2022).

[97] *See* Douglas W. Arner et al., *Stablecoins: Risks, Potential and Regulation* 4-5 (Bank for Int'l Settlements Working Paper, No. 905, 2020).

[98] Auer et al., *supra* note 82*,* at 6.

[99] *E-Krona*, RIKSBANK, https://www.riksbank.se/en-gb/payments--cash/e-krona/ (last visited Feb. 5, 2023).

[100] *E-Krona Pilot Phase 2*, RIKSBANK, https://www.riksbank.se/en-gb/payments--cash/e-krona/e-krona-reports/e-krona-pilot-phase-2/ (last visited Feb. 5, 2023).

Payment ("DC/EP") pilot project in 2020. This project is, by far, the largest CBDC pilot, which has accumulated 360 million pilot transactions amounting to RMB 100.05 billion (equivalent to USD 14.74 billion) as of August 2022.[101] Other major economies, including India and Russia, have started their CBDC pilots. The United States, the United Kingdom, and the European Union are also assessing the issuance of CBDCs. Likely, we will shortly see more sovereigns give life to CBDCs and use them for retail purposes in a scalable manner.

Major economies generally have a consensus that CBDCs should be efficient, convenient, secure, interoperable, and easily accessible. Moreover, CBDCs should be designed to minimize their impact on the existing financial system. They should refrain from excessively competing with bank deposits, e-money, and other payment instruments issued by commercial banks or private companies. Therefore, central banks generally encourage the private sector to incorporate CBDCs into their existing payment applications. They also recognize the significant role cash plays in societies and do not intend to phase out or replace cash even if a cashless society makes a negative interest rate policy available.[102] Ideally, central banks shall minimize CBDC's impact on the financial system, maintain financial and monetary stability, and embrace innovation while ensuring safety.[103]

2. CBDCs: A Challenging Mandate for Central Banks

CBDCs bring a set of challenging tasks to central banks. Central banks receive the mandate to develop and facilitate the operation of CBDCs. This mandate includes the design of a secure and reliable CBDC that prevents counterfeit digital money, a fully operational CBDC system that maintains and verifies transactions, an electronic payment system that accommodates different payment platforms developed by PSPs, a mechanism that effectively enforces AML/CFT regulations, and a system that ensures safe and secure cross-border payment.[104]

Building a CBDC system further requires horizontal coordination between different government agencies. It would bring together managers of national ID schemes, financial supervisors, and cybercrime investigation agencies.[105] It may also include national security agencies, trade and

[101] People's Bank of China's Institute for Digital Currency, *supra* note 7.

[102] In fact, the coexistence of cash and CBDC is also a commonly recognized principle by many sovereigns. BANK OF CAN. et al., *supra* note 4, at 10.

[103] *Id.*

[104] *See* Agustín Carstens, General Manager, Bank for Int'l Settlements, Central Bank Digital Currencies: Putting a Big Idea into Practice, Remarks at the Peterson Institute for International Economics discussion on Central Bank Digital Currencies (Mar. 31, 2021), https://www.bis.org/speeches/sp210331.htm.

[105] Ayang Macdonald, *Digital ID, KYC Infrastructure Critical for Digital Currency Rollout, Says IMF*, BIOMETRIC UPDATE (June 30, 2022), https://www.biometricupdate.com/

investment agencies, public transportation departments, and social welfare departments. Among these government agencies, central banks are likely to take the responsibility of designing CBDC regulatory frameworks. It is less doubtful that CBDC development has become part of central banks' mandates.[106] Other agencies and departments are expected to accommodate their policies to CBDCs and establish regular contact with central banks to facilitate their assigned duties.

CBDCs also bring significant changes to the financial system. The two-tier CBDCs, as illustrated above, require commercial banks, PSPs, and other third-party service providers ("TSPs") to cooperate with central banks. These partnering intermediaries will develop account management and user interface and play a role in user and transaction data protection.

Such an enormous cooperation project requires central banks to consider how CBDCs will accommodate the mandates of different public and private institutions. Central banks thus take a principal role in coordinating the different needs of these institutions. In other words, CBDCs development not only involves building a reliable system but also requires a governance structure surrounding the distribution and application of CBDCs. The scope of such governance might expand the mandate of central banks and connect central banks to other non-monetary policy objectives.

On the other hand, since central banks' CBDC mandate intersects or overlaps with other government authorities' mandates, this creates room for the executive branch to interfere with central bank decisions. The executive branch has the incentives to interfere. As mentioned above, governments increasingly intervene in central bank decisions and compromise their independence. CBDCs' emergence might exacerbate the power struggle between political leaders and central banks. Government intervention would foreseeably complicate the CBDC governance as governments may not have aligned interests with central banks on various issues concerning the use of CBDC.

C. CBDC's Achilles Heel: Privacy Concerns

CBDCs' privacy concerns may serve as a battlefield for the power struggle between political leaders and central banks. Specifically, CBDCs allow central banks to observe, monitor, and even control cash flow more effectively. Central banks may thus identify users and further track and analyze their transaction records based on their CBDC data. While central

202206/digital-id-kyc-infrastructure-critical-for-digital-currency-rollout-says-imf.

[106] Central banks' tasks are directly related to CBDCs. Sovereigns that are interested in CBDCs assign central banks or their branch organizations to conduct research and test of CBDCs. For central banks' role in CBDC governance, *see* Marianne Bechara et al., *The Impact of Fintech on Central Bank Governance* (IMF Fintech Notes, No. NOTE/2021/001, 2021).

banks usually do not need user data to achieve their mandates, other government agencies may find the data useful. The privacy concern is not only about how central banks manage user data but also about central banks' partnership with other agencies.

1. CBDCs and the Inevitable Privacy Implications

Technologically, a central bank may choose to design its CBDCs in a manner free from privacy implications. In practice, however, for various policy purposes, central banks would refrain from adopting such a CBDC design. Below we explain their rationales and the resulting privacy implications of CBDCs.

i. CBDCs' Design Choices and Privacy Implications

CBDCs' design is highly flexible. Central banks may choose the CBDC designs to accommodate the need for digitalization and to improve financial inclusion. For instance, CBDCs have the advantage of allowing central banks to effectively track cash flow to combat the illicit use of money, prompt more effective monetary policies, and help governments distribute or redistribute resources more efficiently.[107] Under certain designs, central banks can further stop, if not revert, illicit transactions, which allows users to retrieve stolen CBDCs. They may also restrict the use of CBDCs to achieve policy objectives.

The "programmability" of CBDCs further suggests that it is technologically feasible to limit the amount, duration, locations, and payees when people use CBDCs.[108] This CBDC feature allows central banks to issue a special type of CBDC only applicable under designated circumstances. This special type of CBDC is particularly useful for government services such as welfare policies because only the target groups receive the CBDC, and the government can ensure the CBDC is used for the intended purpose. Therefore, a government may substitute programmed CBDCs for government-issued vouchers designed for specific purposes.[109]

---

[107] ANTON DIDENKO & ROSS BUCKLEY, ASIAN DEVELOPMENT BANK, CENTRAL BANK DIGITAL CURRENCIES: A POTENTIAL RESPONSE TO THE FINANCIAL INCLUSION CHALLENGES OF THE PACIFIC 21-27 (2021).

[108] Alexander Lee, *What is Programmable Money?*, FEDS NOTES (June 23, 2021), https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html. *See also* Ingo Weber & Mark Staples, *Programmable Money: Next-generation Blockchain-based Conditional Payments*, 4 DIGIT. FIN. 109 (2022); Erwin Kulk & Petra Plompen, *Demystifying Programmable Money: How the Next Generation of Payment Solutions can be Built with Existing Infrastructure*, 15 J. PAYMENTS STRATEGY & SYS. 445 (2021).

[109] There is a distinction between programmable money and programmable payments. CBDC has the potential to enable both. *See* Jonas Gross et al., *Designing a Central Bank Digital Currency with Support for Cash-Like Privacy*, (2021), https://papers.ssrn.com/abstract=3891121.

For instance, a government may issue credits in CBDCs that can only be used to reserve hotels, which is a more efficient tool to bail out the tourist industry than government-issued vouchers. Central banks or governments can further decide how and where certain CBDCs are applicable based on the types of government services. They can also block transactions when there are signs of illicit activities. Central banks will thus have a role in credit and resource redistribution, a task usually bestowed upon governments. In practice, the government may provide guidance to central bankers by creating a list of services and rules. Central banks would then be responsible for setting up the CBDC system to achieve the government's policies.

To reap the above benefits, central banks require identification during CBDC transactions. CBDCs' identification requirements create privacy concerns that are very different from physical cash. Physical cash is entirely anonymous. Therefore, there is no record of who owns or transacts the said cash. In contrast, CBDC's ownership and transaction records are usually kept in data servers administered by central banks.[110] Central banks may further decide what information to preserve, how long it will be preserved, and who can access data under what circumstances when designing CBDCs. Central banks' power over CBDC records inevitably triggers privacy concerns.

The level of CBDCs' privacy concerns varies by different architectural designs. The central bank undoubtedly undertakes the primary privacy protection duty in one-tier CBDCs, where the central bank directly holds all CBDC data. Even in two-tier CBDCs, under which the central bank delegates most CBDC operational tasks to partnering intermediaries, it is not free of the privacy protection duty.[111] As will be illustrated later, if a central bank chooses intermediated CBDCs, under which it merely holds wholesale data and leaves retail data in the hands of partnering intermediaries, its privacy protection duty might be less. That said, it remains obliged to supervise the privacy protection measures of the delegated partnering intermediaries. On the contrary, if a central bank chooses hybrid CBDCs, under which it receives and consolidates the retail CBDC data from partnering intermediaries, its privacy protection duty remains.[112] So is the case with the variant of one-tier CBDCs.

In illustrating CBDCs' privacy concerns, we will start with hybrid CBDCs since it is, by far, the most popular design. Sweden's E-Krona and China's DC/EP, the two primary CBDC pilots, adopt this architectural

[110] Offline transactions still require users to reconnect the server to validate the transaction, which can be called M0.5. *See* David Kuo Chuen Lee et al., *A Global Perspective on Central Bank Digital Currency*, 14 CHINA ECON. J. 52 (2021).

[111] *See generally* Auer & Böhme, *supra* note 36.

[112] *See generally* BANK FOR INT'L SETTLEMENTS INNOVATION HUB & HONG KONG MONETARY AUTHORITY, PROJECT AURUM: A PROTOTYPE FOR TWO-TIER CENTRAL BANK DIGITAL CURRENCY (CBDC) (2022).

design.[113] We will also discuss the central bank's legal responsibility if it delegates the CBDC system or data management services to a professional third party.

ii. The Privacy Implications of Hybrid CBDCs

In hybrid CBDCs, the central bank and partnering intermediaries hold retail CBDC data that involves privacy concerns. In practice, partnering intermediaries are in the front line, being delegated the operational tasks to handle user-facing activities, including account opening, account maintenance, enforcement of AML/CFT rules, and other day-to-day user services. They, therefore, collect and withhold the private information of CBDC users, such as their names, locations, online identifiers, contact information, CBDC balance, CBDC transaction histories, and other information specific to a CBDC user's economic or social identity. They shall undertake privacy protection duties.

Furthermore, the central bank similarly collects and withholds the above private information. In hybrid CBDCs, partnering intermediaries circulate retail CBDC data to the central bank. In turn, the central bank integrates the data received from each intermediary into a consolidated retail CBDC ledger. To that extent, the central bank's retail CBDC data is more comprehensive than any individual intermediary. Based on this information, it possesses the capacity to profile each CBDC user, that is, evaluate certain personal aspects relating to a CBDC user, such as their economic situation, personal preferences, behavior, location, or movements. Profiling allows the central bank to infer further the overall wealth, transaction history, personal preferences, and social, economic, and even political activities of each CBDC user. A government with such capacity can evolve into a surveillance state that monitors and controls each CBDC user's activities, which triggers a severe human rights concern. The central bank shall undoubtedly undertake the privacy protection duty to mitigate this concern.

To complicate the situation, whether the central bank should further undertake a vicarious duty for partnering intermediaries is unclear. In a typical outsourcing relationship, under which an outsourcing bank delegates an outsourced third party to perform certain bank businesses or activities, the central bank typically bears the ultimate responsibility for any misconduct of the outsourced third party.[114] However, similar regulatory logic does not necessarily apply to the delegation relationship between the

[113] Auer et al., *supra* note 82, at 22-24.

[114] For how outsourcing regulation works and how should it be redesigned, *see* Cheng-Yun Tsang, *From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech*, 2019 U. ILL. J.L. TECH. & POL'Y 355, 355-404 (2019). *See also* Luca Enriques & Wolf-Georg Ringe, *Bank-Fintech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime*, 15 CAP. MKTS. L.J. 374 (2020).

central bank and partnering intermediaries in hybrid CBDCs. It, therefore, begs the question of to what extent the central bank should undertake the privacy protection liability caused by partnering intermediaries. In any event, the central bank shall at least establish regulatory measures to supervise the privacy protection measures of these intermediaries and hold them accountable for any privacy breach, data abuse, or privacy infringement caused. This supervisory oversight involves clarifying the existing legal framework and establishing institutional check-and-balance.

On the other hand, given the concern of financial stability, AML/CFT, fraud and theft, and other potential illicit uses of CBDC, it is widely accepted that central banks are justified to retain the ability to trace and monitor CBDC transactions.[115] Hybrid CBDCs may satisfy this need. Although partnering intermediaries take charge of the KYC process and most user-facing activities, central banks keep the consolidated retail CBDC ledger that records all retail CBDC data. Therefore, central banks retain the ability to access and analyze the related data to facilitate the above justifiable policy purposes.

Even if the central bank commit to dis-identifying user information to keep the privacy commitment, this commitment alone does not eliminate the possibility for them or other governmental agencies, such as law enforcement and intelligence agencies, to re-identify the personal information by piecing together information from other sources.[116] Therefore, while hybrid CBDCs are less anonymous and are thus more of a privacy concern, they might be desirable for pursuing other policy objectives.

2. The Uneasy Task of Privacy Protection

To the extent that central banks cannot and should not eliminate privacy concerns related to CBDCs, the next question becomes how to

---

[115] FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 14, 19-20; TREASURY 2022 REPORT, *supra* note 13, at 26-27, 42-43; Eurogroup, *supra* note 29; Mu, *supra* note 33, at 5. *See also* Daniel Dupuis et al., *Money Laundering in a CBDC World: A Game of Cats and Mice*, 29 J. FIN. CRIME 171 (2021); Kristalina Georgieva, Managing Director, IMF, The Future of Money: Gearing up for Central Bank Digital Currency, Speech at Atlantic Council, Washington, DC (Feb. 9, 2022), https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency.

[116] China's digital Yuan is a significant example. The People's Bank of China has access to transaction data even under the so-called "managed anonymity" or "controllable anonymity," *see* Martin Chorzempa, *Promise and Peril of Digital Money in China Digital Currencies: Risk or Promise?*, 41 CATO J. 295, 301-303 (2021); Nir Kshetri, *China's Digital Yuan: Motivations of the Chinese Government and Potential Global Effects*, 32 J. CONTEMP. CHINA 87 (2022); James Kynge & Sun Yu, *Virtual Control: The Agenda Behind China's New Digital Currency*, FIN. TIMES (Feb. 16, 2021), https://www.ft.com/content/7511809e-827e-4526-81ad-ae83f405f623; Brenda Goh & Samuel Shen, *China's Proposed Digital Currency More about Policing than Progress*, REUTERS (Nov. 1, 2019), https://www.reuters.com/article/us-china-markets-digital-currency-idUSKBN1XB3QP.

discipline central banks to reduce privacy concerns to a tolerable level that can be managed.

Disciplining central banks from a privacy perspective entails certain legal designs. For instance, under what conditions are central banks permitted or even required to process CBDC data or share the data with other governmental agencies? How should a central bank ensure that it will follow the privacy protection requirements, such as the legitimate use, the minimization principle, and the internal control requirement? Modern privacy laws, such as the General Data Protection Regulation ("GDPR") in the European Union or the California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA") in California, the United States, lay down comprehensive sets of privacy laws imposed on private businesses, which sometimes extend to public authorities. They may similarly apply to issuing central banks and their partnering intermediaries, rendering privacy protection challenging for central banks. Below we illustrate the challenges of data protection and data security aspects.

i. Central Banks and the Uneasy Task of Data Protection

Central banks are not designed to deal with data, not to mention very sizable data like CBDC data. If a central bank collects, stores, and processes CBDC data, it must implement a well-crafted data governance regime to comply with relevant data protection laws.

Data governance, however, could be beyond a central bank's capacity. Modern data protection laws, such as GDPR,[117] have established a complicated web of principles to govern the processing of personal data, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.[118] Suppose a central bank or any governmental agency attempts to collect or use available CBDC data to pursue certain public functions. In that case, it inevitably engages in personal data processing and shall abide by these principles accordingly. In GDPR's context, issuing central bank's access and processing of personal data will be treated as governmental use of personal data, subject to relevant safeguards.[119] Compliance with these regulations, however, is easier said than done, not to mention that not every sovereign has data protection laws like GDPR.

Take the principle of lawfulness as an example. Suppose a central bank wishes to process CBDC data without obtaining the user's consent. In

[117] For a summary of GDPR, *see generally* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93 (2020).

[118] Regulation 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 (General Data Protection Regulation), art. 5.1, 2016 O.J. (L 119) [hereinafter GDPR].

[119] *See* SANJAY SHARMA, DATA PRIVACY AND GDPR HANDBOOK 287-313 (2020).

that case, modern data protection laws typically require a specific and unambiguous legal mandate that lays down the legal basis for said data processing. [120] In other words, the central bank may not simply resort to the abstract concept of public goods. Without such clear legal mandates, the central bank can only establish the lawfulness of its CBDC data processing by obtaining prior consent from related data subjects. Even in that case, modern data protection laws require informed consent which disqualifies blanket consent by data subjects for the future processing of their data for open-ended purposes.[121] Accordingly, to use CBDC data, the central bank must follow the legal requirements to obtain qualified informed consent, such as specifying the exact uses and purposes of the CBDC data processing in advance.

The central bank must also learn how to establish a robust internal control mechanism to protect privacy. Modern data protection laws impose many internal control requirements upon data controllers, such as the requirements related to records, security, data breach notification, impact assessment, data protection officer, etc. By withholding CBDC data, the central bank needs to implement appropriate technological and organizational measures to ensure that its data processing is in accordance with data protection laws.[122] This is a significant change to the current central bank practice. Currently, central banks only issue physical cash that does not involve personal data and thus need not introduce related internal control measures. To be sure, central banks are not entirely inexperienced in adopting privacy-related internal control measures. That said, the scale of the potential compliance cost is different this time because CBDC is issued to a significant number of people at a substantial amount.

In sum, issues surrounding CBDC data governance are manifold. All require expertise that central banks generally do not have. To make the case even worse, central banks have already suffered from the "distraction disease,"[123] in the sense that they have undertaken too many atypical missions, ranging from traditional mandates, such as ensuring price stability and full employment, to new mandates, such as promoting financial inclusion, tackling climate change, and curing inequality.[124] Given so many

---

[120] GDPR, *supra* note 118, art. 6.3.2.

[121] *Id.*

[122] *Id.* art. 24.1.1.

[123] *See The Danger of Excessive Distraction*, ECONOMIST: CENTRAL BANKS (Apr. 20, 2022), https://www.economist.com/special-report/2022/04/20/the-danger-of-excessive-distraction.

[124] For example, the General Manager of the BIS also recognized the inequality has been a rising concern, but the central banks currently do not have the necessary mandates and tools to achieve targeted distributional outcomes yet. Agustín Carstens, General Manager, Bank for Int'l Settlements, Central Banks and Inequality, Remarks at Markus' Academy, Princeton University's Bendheim Center for Finance (May 6, 2021), https://www.bis.org/speeches/sp210506.pdf . As for whether the central bank should undertake any role in tackling climate changes, major central bankers' views are also

agendas on their plates, central banks do not necessarily have the extra capacity to ensure a robust internal data governance mechanism to safeguard the privacy and security of CBDC data.

ii. Central Banks and the Uneasy Task of Data Security

To maintain a secure and efficient CBDC service, central banks must step into information technology with which they are unfamiliar. Central banks, however, do not necessarily have the extra technological capacity. After all, due to resource and talent constraints, many central banks cannot afford to hire information engineers and data scientists.[125] Therefore, while laws may mandate central banks to be responsible for maintaining and securing the CBDC data, central banks may not have the expertise to tackle the related cyber risk.

Moreover, to the extent that the two-tier CBDCs have become mainstream, the issuing central bank should cooperate with partnering intermediaries. For instance, central banks may have to collaborate with commercial banks or PSPs to conduct KYC and distribute CBDC or engage technology solution providers or TSPs to store, process, and analyze the collected CBDC data.[126] This further complicates the central bank's data management. A glitch or misstep by these partnering intermediaries may fare into a cyber security event or privacy infringement. In that case, it would likely be the central bank's responsibility to clean the mess. To prevent the potential disaster, issuing central banks must know how to prevent, detect, and mitigate such glitches or missteps and possess the necessary mechanism to supervise their partnering intermediaries. Unfortunately, this know-how and skillset are typically not within the central bank's capacity.

3. CBDC's Privacy Concerns and Central Bank Independence

Current studies have generally noted the inherent conflict between privacy and other public policies associated with CBDCs. However, in this paper, we argue that CBDCs' privacy implications are more complicated than that. Specifically, we wish to highlight an additional layer: the inherent conflict between the privacy aspects and central bank independence. We argue that while modern privacy laws may discipline central banks and

---

divergent. *See, e.g.,* Elliot Smith, *Major Central Bankers Dispute Role in Tackling Climate Change as They Battle Inflation*, CNBC (Jan. 11, 2023), https://www.cnbc.com/2023/01/11/major-central-bankers-dispute-role-in-tackling-climate-change-as-they-battle-inflation.html .

[125] Sandra Waliczek & Arushi Goel, *When It Comes to Central Bank Digital Currencies, We Need Public-Private Cooperation*, WORLD ECON. FORUM (May 23, 2022), https://www.weforum.org/agenda/2022/05/cbdcs-the-case-for-public-private-cooperation.

[126] Data management is likely a responsibility of non-bank operators. Peter Wierts & Harro Boven, *Central Bank Digital Currency - Objectives, Preconditions and Design Choices* (De Nederlandsche Bank Occasional Studies, No. 20-01, 2020).

address part of the privacy concerns with CBDCs, they also risk compromising central bank independence.

Maintaining central bank independence has long been a doctrine among the global financial community. This doctrine is based on empirical evidence that central banks work more efficiently with fewer government interventions. Governments are inclined to prefer looser monetary policy, which contradicts central banks' primary objective. Central banks regularly face pressure to pursue short-term political agendas. More independent central banks can better resist these pressures and maintain professional decisions that benefits long-term economic stability. The degree of independence usually rests on the institutional design of central banks. Common measures include tenure protection for central bank governors, an uninterrupted decision-making process, and clear mandates for central banks. Central bank independence minimizes policy volatility. It helps send a clear signal to the market. Independence allows a central bank to exercise its monetary discretion impartially, unaffected by political pressure.[127]

Despite this doctrine's importance, other governmental agencies have always had the motivation to interfere with central banks' operations, as illustrated above. By creating a master ledger containing comprehensive CBDC data, CBDCs create an additional opportunity for derogating central bank independence. Other governmental authorities would be eager to gain access to CBDC data to accommodate their interests or fulfill their duties. They may try to access central bank data or force central banks to collect it. When a government has such access, there is a risk of privacy infringement and potential human rights violations.[128] It may erode central bank independence with the claim that their actions serve public policy objectives and are completely legal. Central bank independence against the need of other governmental agencies becomes the dispute in this scenario.

To be sure, governments worldwide, democracies and authoritarian states alike, are keen to make public commitments to user privacy. Privacy protection has become a priority because the general public cares deeply about anonymity and distrusts the government.[129] But these commitments are likely to be cheap talk. There is little, if any, check-and-balance to

---

[127] For the discussion of central bank independence, *see, e.g.,* Paul Wachtel & Mario I. Blejer, *A Fresh Look at Central Bank Independence*, 40 CATO J. 105 (2020); Kenneth Rogoff, *Is This the Beginning of the End of Central Bank Independence?* (G-30 Occasional Paper, No. 95, 2019); Donato Masciandaro et al., *Central Bank Independence: Metrics and Empirics* (BAFFI CAREFIN Centre Working Paper, No. 151, 2021); Rodolpho Dall'Orto Mas et al., *The Case for Central Bank Independence: A Review of Key Issues in the International Debate* (European Central Bank Occasional Paper, No. 248, 2020); Erik Jones & Matthias Matthijs, *Rethinking Central-Bank Independence*, 30 J. DEMOCRACY 127 (2019).

[128] For the study raising the concern that using CBDC might introduce privacy concerns, *see* Gabriel Soderberg et al., *Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons* (IMF Fintech Notes, No. NOTE/2022/004).

[129] Emanuele Borgonovo et al., *Money, Privacy, Anonymity: What do Experiments Tell Us?*, 56 J. FIN. STABILITY 100934 (2021).

ensure that central banks and their governments will protect user privacy and process CBDC data responsibly. On that note, governments, in effect, may misuse CBDC data and infringe on user privacy because they have an interest in using the CBDC data to fulfill their mandates. Law enforcement, crime prevention, intelligence detection, or even national security can benefit from CBDC data.[130] In brief, the government has an inherent conflict of interest.

When a government chooses to initiate such surveillance and employs its central bank to do so, not every central bank can say no. Admittedly, most major central banks enjoy independence. Nonetheless, as illustrated above, it is not uncommon to see elected politicians demand that central bank governors follow their agenda. When a government requires its central bank to utilize CBDC data, it severely threatens citizens' privacy and jeopardizes the central bank's independence. Admittedly, we have not seen publicized cases where governments misuse CBDC data. After all, the number of active CBDC cases is limited. Nevertheless, one would reasonably expect that a more authoritative political entity, like China, is likely to direct its central bank to achieve political and policy agendas.

Besides, insufficient privacy protection safeguards indeed have led to low public trust in CBDCs. Nigeria, for example, has in place the Nigeria Data Protection Regulation (NDPR) to protect data privacy.[131] and also govern the privacy aspects of its CBDC, eNaira. However, neither the government nor the Central Bank of Nigeria have sufficiently robust institutions to enforce NDPR. The public trust in the government's capacity to protect personal data, thus, remains low. Analysts have pointed out that the privacy concern is one of the main reasons resulting in low eNaira adoption.[132]

The problem can be more acute if a CBDC is programmable. For instance, if a government were to dissuade a mass protest, it might limit the CBDC transactions around the protest location; it may track protesters' footprints using public transportation records; it may disable protesters' e-wallets; it may anticipate violent behaviors based on the transaction records of the protesters. CBDCs provide government agencies with a tool to

---

[130] Nerenda N. Atako, *Privacy beyond Possession: Solving the Access Conundrum in Digital Dollars Notes*, 23 VAND. J. ENT. & TECH. L. 821 (2020).

[131] Kemi Omotubora & Subhajit Basu, *Nigeria's eNaira Faces a Bunch of Privacy Challenges*, THE REGISTER (Nov. 22, 2021), https://www.theregister.com/2021/11/22/e_naira_legal_privacy/ (last visited Jun 8, 2023). *See also* Olumide Babalola, *Nigeria's Data Protection Legal and Institutional Model: An Overview*, 12 INT'L DATA PRIVACY L. 44 (2022).

[132] Gbenga Odugbemi, *An Evaluation of Nigeria's National Identity Management Commission "MWS Mobile ID App", and the Central Bank of Nigeria's "e-Naira Speed Wallet App" from a Privacy Perspective*, (Dec. 29, 2021), https://papers.ssrn.com/abstract=3994919 (last visited Jun 8, 2023); Kelechukwu Iruoma, *ANALYSIS-Got your number: Privacy concerns hobble Nigeria's digital ID push*, REUTERS (Aug. 5, 2021), https://www.reuters.com/article/nigeria-tech-rights-idUSL8N2OW2CJ (last visited Jun 8, 2023).

perform their tasks more efficiently. These agencies can hardly say no to utilizing this tool if circumstances permit,[133] including by compromising the central bank's independence.

Central banks are not mandated to address national security or enforce AML/CFT. They also do not possess the expertise to facilitate national and foreign policy objectives. These are the mandates of other governmental agencies. That said, other governmental agencies would have the motivation to reach these goals by utilizing the CBDC data withheld by the central bank. When these governmental agencies request the participation of central banks, central banks are not necessarily capable of keeping their promise of user privacy, albeit for seemingly legitimate reasons.

4. Summary

In sum, CBDCs open Pandora's Box, which exhibits the struggle among privacy protection, other public policy objectives, and the long-lasting principle of central bank independence. This additional central bank independence concern complicates the CBDC design in two aspects. On the one hand, the rising use of CBDCs may erode central bank independence and turn central banks into rather politically oriented machines. Specifically, given the abundant value of CBDC data, we predict that other governmental agencies will tend to force central banks to intervene in issues they do not necessarily have the mandate or capacity to tackle. On the other hand, we argue that the potential misuse of CBDC data by central banks still warrants some privacy disciplines upon central banks. However, imposing these privacy laws upon central banks opens a gate to compromising central bank independence.

Among the growing literature on CBDCs, we see a gap in such discussions and a surprisingly light-touch focus on the grave issue of privacy concerns with CBDCs. We aim to fill this gap by highlighting the importance and urgency of rethinking privacy concerns in the context of CBDCs and proposing potential solutions to address these concerns in the next section.

III. DISCIPLINING CBDC'S PRIVACY CONCERNS FROM A DOMESTIC PERSPECTIVE

The privacy issue of CBDCs is notable, but it is not something that cannot be addressed. In this section, we discuss several CBDC models proclaimed to mitigate the privacy concerns of CBDCs and recognized by

[133] For similar observations, *see* Jeremy Light, *The Risks to Society of Central Bank Digital Currencies*, FINEXTRA RESEARCH (Jan. 17, 2022), https://www.finextra.com/blogposting/21584/the-risks-to-society-of-central-bank-digital-currencies; Sofie Blakstad & Robert Allen, *Central Bank Digital Currencies and Cryptocurrencies*, *in* FINTECH REVOLUTION: UNIVERSAL INCLUSION IN THE NEW FINANCIAL ECOSYSTEM 87 (Sofie Blakstad & Robert Allen eds., 2018).

regulators as capable of dealing with privacy concerns. We argue that these tools cannot function on their own; instead, states need to adopt proper institutional monitoring mechanisms to make these tools credible. On that basis, we further discuss how domestic laws may be designed to address the privacy concerns associated with CBDCs, particularly the central bank independence aspect.

A. The Limits of Available Proposals

Studies and practices have noted privacy concerns with CBDCs and proposed corresponding measures. Well-known examples include complying with the existing privacy laws, partially anonymizing CBDCs, token based CBDCs, and intermediated CBDCs. We will discuss the limits of these proposals in this subsection.

1. Undertaking the Privacy Protection Duties

The simplest, and perhaps the most common, way for central banks to address CBDC's privacy concerns is to comply with privacy laws. Most central banks choose to undertake the privacy protection obligations imposed by existing privacy laws and introduce necessary protective measures. They might be willing to undertake it, particularly if they determine that the expected benefit from CBDCs surpasses the compliance cost.[134]

The concern with this approach is credibility. As mentioned above, central banks might not possess the necessary expertise and capacity to undertake these duties. Their motivation to comply with privacy protection laws might be weak. Central banks in some sovereigns might even claim the protection of state immunity.[135] These all beg the question of how to establish a credible disciplinary regime against central banks.

Take the famous GDPR, for instance. GDPR's regulatory obligations may extend to governmental agencies, including central banks.[136] Therefore, the issuing central bank's collection, processing, and use of personal data will fall under GDPR's purview. GDPR further requires member states to establish an independent supervisory agency (*e.g.*, Data Protection Authorities) that may oversee the central banks' CBDC-related

[134] For studies arguing that issuing central banks would not have much problem complying with their privacy protection obligations, *see* Crawford et al., *supra* note 23, at 164-67.

[135] Privacy protection laws in some jurisdictions do not extend to public authorities. For instance, the famous CCPA and CPRA, considered the most comprehensive privacy regulations in the United States, only apply to "businesses" and therefore do not extend to governmental authorities. California Privacy Protection Agency, *Frequently Asked Questions (FAQs), Question 4*, https://cppa.ca.gov/faq.html (last visited Oct. 7, 2023) [hereinafter CPPA].

[136] SHARMA, *supra* note 119, at 288.

activities and compliance.[137] It seems encompassing enough to discipline CBDCs' privacy concerns.

That said, GDPR also allows member states to exercise a certain degree of customization through the so-called "opening clauses," which would enable a member state to modify GDPR provisions in which the clause resides. Therefore, those non-Euro area member countries[138] may design their CBDCs with fewer GDPR constraints. This delegation makes it challenging to predict whether a member state will forcefully require an issuing central bank to comply fully with the regulations.[139]

Furthermore, GDPR also incorporates a set of exceptions to many rules provided that data processing is performed in the public interest.[140] Under EU laws, public interest involves a member state's financial or economic policy.[141] Such an exception, accompanied by a clear legal mandate, may easily relieve a CBDC-issuing member state from many GDPR obligations. Central banks of these member states may, thus, process CBDC data based on these legal mandates instead of data subjects' consent without being treated as an infringement of their citizens' privacy rights.

Last but not least, even if a member state does not choose to opt out of its GDPR obligations, the enforcement problem remains. To what extent the data protection authority of a member state will enforce the data protection regulations when confronting its central bank, a long-considered independent authority, requires further observation.

2. Anonymizing or Deidentifying the CBDC Data as a Way Out?

Modern privacy laws do not extend to processing anonymous data, that is, personal data whose data subject is no longer identifiable.[142] Therefore, some central banks might wish to anonymize or deidentify the CBDC data to be free from privacy protection duties.

Data anonymization or deidentification, however, is a challenging task. In general, it requires the absence of any reasonably likely means to be used by any person to identify the natural person directly or indirectly.[143] In other words, fully anonymized CBDC data means that no one can identify the exact CBDC user of a given CBDC account. However, for one thing, fully anonymizing or deidentifying the CBDC data would impair the

---

[137] *Id.* at 241-49.

[138] Currently, six EU member states, Bulgaria, Czechia, Hungary, Poland, Romania, and Sweden, are not Euro area countries. *Countries Using the Euro*, EUROPEAN UNION, https://european-union.europa.eu/institutions-law-budget/euro/countries-using-euro_en (last visited Feb. 7, 2023).

[139] SHARMA, *supra* note 119, at 288.

[140] *Id.* at 291.

[141] *Id*.

[142] *See, e.g.*, GDPR, *supra* note 118, Recital 26.5 and 26.6.

[143] *Id.* Recital 26.3.

operation of CBDCs because no one can identify the payer and payee in the transaction to complete CBDC payments. Besides, it also increases the risk of illicit use of CBDCs. Therefore, as illustrated above, the consensus among world central banks is that CBDCs cannot be as anonymous as physical cash in light of several public purposes such as AML/CFT.[144] Hence, completely anonymizing or deidentifying the CBDC data to avoid the application of privacy laws is not a feasible solution.

Some central banks, in practice, pseudonymize instead of anonymize the CBDC data.[145] The hybrid structure adopted by Sweden's e-Krona project is a good example. Sweden's central bank, Riksbank, is conscious of CBDC's privacy concerns. Therefore, it introduced a special design under which the identity of CBDC users is only known to partnering intermediaries responsible for the KYC and ongoing due diligence. Notably, the identity of CBDC users is unknown to Riksbank. Riksbank only receives information from the intermediaries on individual account balances and payments, but it does not receive any information on the actual account holders.[146] This design prevents Riksbank from identifying CBDC users directly.

However, e-Krona's design, at most, pseudonymizes, instead of anonymizing, CBDC data. After all, Riksbank can still identify CBDC users with the additional information withheld by partnering intermediaries. Therefore, by receiving information on individual account balances and payments, Riksbank still collects personal data and constitutes a data controller subject to data protection laws.[147]

3. The Myth of "Token-Based CBDC"

We then wish to demystify the alleged privacy-proof function of the so-called "token-based CBDC." As illustrated above, many CBDCs adopt the so-called "account-based" system that allows central banks to access the information of users' transaction accounts. Under this design, each CBDC user must apply for a CBDC account to conduct CBDC transactions. Through the KYC process for opening a CBDC account, partnering intermediaries know the identity of each CBDC user, which triggers privacy concerns between CBDC users vis-à-vis partnering intermediaries.

---

[144] *See, e.g.*, FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 13-14; Eurogroup, *supra* note 29; Mu, *supra* note 33, at 5; BANK OF CAN. ET AL., *supra* note 4.

[145] China, for instance, claims that it permits anonymity for small-amount CBDC transactions and designs the so-called Level Four wallets to serve as anonymous wallets for that purpose. However, to open the Level Four wallets, users still need to provide a phone number, which may identify a specific person if combined with the identify information held by telecom operators. Mu, *supra* note 33, at 3-4. Therefore, this design, at most, pseudonymize the digital yuan data.

[146] *See* Auer et al., *supra* note 82, at 25.

[147] That said, by pseudonymizing the CBDC data, Riksbank is more likely to satisfy the data controller obligation such as privacy-by-design and privacy-by-default.

Moreover, the problems may be escalated to those between CBDC users vis-à-vis central banks if partnering intermediaries further circulate the information to central banks in the variant of one-tier CBDCs or hybrid CBDCs.

Some commentators advocate that token-based CBDCs may address privacy concerns as they function similarly to digital cash.[148] By definition, token-based CBDCs refer to CBDCs that are "secured via passwords such as digital signatures that can be accessed anonymously."[149] It is generally believed that token-based CBDCs adopt a cash-like design that gives individual users access to the CBDC based on a password (e.g., digital signature using private-public key cryptography) without requiring personal identification.[150] Token-based CBDCs may further support the offline transaction viability of CBDCs, which additionally gives users some transactional anonymity.[151] Appealed by the anonymity feature of token-based CBDCs, some central banks appear to favor a hybrid of account-based and token-based CBDCs.[152] For instance, smaller CBDC transactions may be done in token-based CBDCs, which permit offline transactions that do not require identification.[153]

However, the anonymity feature and the associated privacy-proof function of token-based CBDCs are exaggerated. This exaggeration results from the misleading use of the term "anonymous" when defining token-based CBDCs. "Anonymous" is a polysemous term. Modern privacy laws define anonymous based on the strict distinction between the concepts of "identified" and "identifiable." If the subject(s) regarding certain information is not directly identified but may be attributed to a natural person by using additional information, they remain identifiable, and the subject(s) will be treated as Data Subject(s).Thus, the information is merely pseudonymous instead of anonymous and remains within the ambit of privacy laws.[154]

As illustrated above, CBDCs cannot be anonymous in this strict sense.

---

[148] *See, e.g.*, Gina Ahmar, *Digitizing the Dollar: Privacy Considerations and Policy Prescriptions for a U.S. Central Bank Digital Currency*, 18 HASTINGS BUS. L.J. 149 (2021). Thrasher, *supra* note 35; Christian Grothoff & Thomas Moser, *How to Issue a Privacy-preserving Central Bank Digital Currency* (SUERF Policy Brief, NO. 114, 2021).

[149] BIS 2021 ANNUAL REPORT, *supra* note 36, at 92.

[150] *Id.* at 72.

[151] Being offline, however, does not mean complete anonymity, *see* Ye Wang et al., *Print Your Money: Cash-Like Experiences with Digital Money* (2021), https://arxiv.org/pdf/2104.10480.pdf; Gross et al., *supra* note 109.

[152] China's digital yuan adopts this idea and permits "anonymous" CBDCs for small-amount transactions. Mu, *supra* note 33, at 3-4. Sweden is also reportedly surveying this possibility. Auer et al., *supra* note 82, at 24-25. The European Union also seems to favor this idea. *Lagarde: 'Low-Value, Low-Risk' Digital Euro Payments Could Be Anonymous*, *supra* note 35.

[153] BIS 2021 ANNUAL REPORT, *supra* note 36, at 72.

[154] *See, e.g.*, GDPR, *supra* note 118 Recital 26.

The same applies to token-based CBDCs. The "anonymity feature" claimed by advocates of token-based CBDCs is, at most, pseudonymous under modern privacy laws. When BIS uses "anonymous" to describe token-based CBDCs, it refers to the absence of an identification scheme that identifies the personal identity of CBDC users. In this sense, BIS uses "anonymous" only to refer to the fact that users of token-based CBDCs are not "identified."

However, that alone is not enough to relieve the privacy concerns associated with token-based CBDCs because their users remain "identifiable." The issuance and circulation of token-based CBDCs still require basic KYC procedures and information.[155] While various CBDC pilot programs claim that their designs ensure the anonymity of their users, they require users to use mobile phone numbers to access CBDCs.[156] Even offline CBDCs need a device, most likely a cellphone.[157] Moreover, in the variant of one-tier CBDCs or hybrid CBDCs, after being connected to the web, the offline transaction records of these token-based CBDCs will eventually be documented in the central bank's CBDC ledger. In sum, CBDCs inevitably implicate identification, and token-based CBDCs are not free from such identification requirements.[158]

Some may well argue that as long as the information related to the identity of CBDC users (e.g., mobile number, email address, etc.) is merely placed at partnering intermediaries and does not flow to the issuing central bank, these CBDCs will not incur privacy concerns.[159] This argument essentially advocates using the so-called "intermediated CBDCs," which leads us to the next discussion.

4. The Potential of Intermediated CBDCs

Another potential method for central banks to address CBDCs' privacy concerns is intermediated CBDCs. As mentioned above, the Federal Reserve of the United States appears to favor this design. The essence of this structure is that central banks delegate the task of ledger administration to partnering intermediaries and do not hold a consolidated CBDC ledger.

---

[155] Soderberg et al., *supra* note 128 at 10-11.

[156] For instance, China states that its digital yuan permits anonymous wallets to support the principle of "anonymity for small amounts, traceability for large amounts." However, these Level-four wallets still require a phone number to be opened. Mu, *supra* note 33, at 3–4. This operation reveals that China's "anonymous wallets" design is, at most, pseudonymous.

[157] *See* John Kiff, *Taking Digital Currencies Offline*, IMF (Sept. 2022), https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline.

[158] For related criticism of token-based CBDCs, *see* Crawford et al., *supra* note 23, at 150-55.

[159] China, for instance, emphasizes that its Personal Information Protection Law prevents telecom operators from arbitrarily disclosing the identity information behind the mobile phone numbers to third parties, including the central bank. Mu, *supra* note 33, at 3-4.

This structure contains two steps. As the first step, a central bank issues the CBDC to its partnering intermediaries on a wholesale basis. At this stage, the central bank possesses the information related to the CBDC holding of these partnering intermediaries. This information, however, is merely attributed to these partnering intermediaries, which are legal persons rather than natural persons. Therefore, the issuing central bank itself has not triggered privacy concerns.

As the second step, the partnering intermediaries distribute the issued CBDCs assigned to public CBDC users. At this stage, partnering intermediaries inevitably withhold CBDC data whose data subject is identifiable and, thus, shall comply with associated privacy protection obligations. However, this move does not impose privacy protection obligations upon the issuing central bank as long as the partnering intermediaries do not circulate the CBDC data to the central bank.

Under this design, the issuing central bank cannot administer a consolidated CBDC ledger because it does not have the data attributed to each CBDC user. Instead, it merely possesses the CBDC data attributed to partnering intermediaries on a wholesale basis. Only the partnering intermediaries possess the data attributed to public CBDC users. To that extent, privacy concerns do not exist between CBDC users vis-à-vis central banks. Privacy laws, if applicable, apply only to partnering intermediaries and would not extend to the central bank.

Intermediated CBDCs essentially replicate the current cash- and deposit-based payment system.[160] Under the current system, the central bank engages in the payment system by issuing physical cash on a wholesale basis to designated banks and operating the reserve ledger documenting the reserve data of banks. Neither engagement, however, triggers data protection obligations. Banks, in turn, possess the deposit information attributed to public depositors and thus undertake the associated data protection duties. Banks, however, do not pass the information of their depositors to the central bank, which reduces the privacy concerns at the central bank end. Intermediated CBDCs borrow this logic. The difference is that under the current payment system, banks operate deposit accounts representing depositors' claims against banks. In contrast, under the intermediated CBDCs, banks and other partnering intermediaries operate CBDC accounts on the central bank's behalf, representing direct claims of CBDC users against the central bank.

Central banks' primary concern in adopting intermediated CBDCs is that they no longer administer a consolidated CBDC ledger. This

[160] For a discussion of the modern payment system, *see* Anton N.Didenko & Ross P.Buckley, 87*The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies*, 42 FORDHAM INT'L L.J. 1041 (2019). For a historical account of this system, *see generally* Isabel Schnabel & Hyun Song Shin, *Money and Trust: Lessons from the 1620s for Money in the Digital Age* (Bank for Int'l Settlements Working Paper, No. 698, 2018).

compromises several CBDC functions. For instance, the money flow cannot be as transparent as envisaged because this structure fragments the CBDC ledger. The clearing and settlement of CBDC payments would be less disintermediated because partnering intermediaries would play a more significant role in intermediating the CBDC payment. The implementation of bailout measures or monetary measures cannot be as targeted as envisaged because the CBDC information possessed by the central bank is not individualized enough. We believe that a central bank thus needs to assess whether this tradeoff is cost-efficient.[161]

Current studies have further noticed several potential concerns of intermediated CBDCs. For instance, to the extent that central banks do not keep the latest records of CBDC users, they may lack information to perform their duties when relevant partnering intermediaries run into problems. Therefore, intermediated CBDCs require some additional traceability solutions.[162] For instance, central banks might need to supervise partnering intermediaries to ensure that each intermediary's wholesale holdings reported to them accurately reflect its CBDC users' retail holdings.[163]

Current studies and some sovereigns (like the United States) appear optimistic about intermediated CBDCs as an effective structure to control CBDC privacy concerns. We are, however, less optimistic. It begs the fundamental question of a sovereign's power and will. Whether a monarchy or a democracy, governments monitor and control citizens to maintain their power and legitimacy. Therefore, the credibility of an intermediated CBDC cannot be built on the central bank's unilateral declaration. After all, a CBDC's actual operation is inherently opaque. Whether the partnering intermediaries circulate the data of CBDC users to the central bank or other governmental authorities is particularly unclear to the public. For instance, one can hardly imagine that a partnering intermediary would say no to its central bank or other governmental authorities should they request the information for legitimate reasons. If that is the case, there remains a possibility that a government can utilize CBDC data to monitor CBDC users if it wants.[164] Such a Levitan-style assumption is not remote, as

---

[161] Some studies have noted that a critical national policy question related to CBDC is deciding who can access which parts of CBDC information and under what circumstances. This question involves a balance between public privacy (especially as data protection legislation continues to evolve) and reducing illegal activity. BANK OF CAN. ET AL., *supra* note 4, at 6.

[162] HKMA, *supra* note 53, at 15. *See also* Auer & Böhme, *supra* note 36, at 12.

[163] BIS 2021 ANNUAL REPORT, *supra* note 36, at 79.

[164] China may present an interesting case. China officially declares that its digital yuan adopts a two-tier operating system, under which its central bank "only processes inter-institutional transaction information and does not hold personal information." On its face, China's digital yuan seems to adopt an intermediated CBDC model. Mu, *supra* note 33, at 2. However, this position does not seem to be well received by the international community. Some studies report that China's central bank "periodically receives and stores a copy of

governments have an abundant history of abusing data.[165]

Therefore, to credibly eliminate privacy concerns, an intermediated CBDC must not only deal with the inherent tradeoffs noted by the current studies. It must further introduce a credible mechanism that prevents partnering intermediaries from circulating the information to central banks and other governmental authorities. Even intermediated CBDCs cannot realize the proclaimed privacy protection advantage without this credible mechanism.

B. Designing a Credible Disciplinary Regime

In the previous sub-section, we discussed the privacy protection limits of four potential models. The bottom line is that for each to realize the proclaimed privacy protection function, it requires a credible disciplinary mechanism to ensure that its implementation follows the design. This, in turn, begs the fundamental question of how a domestic regulatory system may effectively supervise and govern central banks and other governmental authorities to alleviate the privacy concerns between CBDC users vis-à-vis the government.

While achieving that goal would be difficult, it is not entirely impossible. In this subsection, we propose three potential solutions in the domestic context: *ex-post congressional oversight*, *special independent supervisory institutions*, and *tailor-made data protection regimes*. Below we present a brief explanation of these three proposed solutions. Each solution requires rethinking the following three broad questions: first, can a central bank handle big data and ensure privacy safeguards? What if it cannot? How can it be made possible? Second, who has the power and capability to effectively supervise central banks' compliance with the data protection laws and regime? Can a data protection authority undertake that mission? How can the existing data protection law apply to a central bank? Third, would that contradict the principle of central bank independence if there is a supervising agency to oversee the central bank? How can we reconcile both objectives?

1. Ex-post Congressional Oversight

The first possible solution is to resort to democratic checks-and-balances. This solution is built on the assumption that the issuing central

---

retail holdings and transactions" and thus classify China's digital yuan as adopting a hybrid CBDC model. Auer et al., *supra* note 82, at 22-23. *See also* BIS 2021 ANNUAL REPORT, *supra* note 36, at 79.

[165] For arguments and counterarguments of how the world had become an administrative state and whether there is any cure, *see generally* CASS R. SUNSTEIN & ADRIAN ZERMEULE, LAW AND LEVIATHAN: REDEEMING THE ADMINISTRATIVE STATE (2020); David Ballaschk & Jan Paulick, *The Public, the Private and the Secret: Thoughts on Privacy in Central Bank Digital Currencies*, 15 J. PAYMENTS STRATEGY & SYS. 277 (2021).

bank will be forced to "line up" with the executive branch of the government. Therefore, only legislative oversight would have sufficient power to balance that political pressure. In democracies, congress often plays many policy-shaping and agency-overseeing roles. Congress can form a committee, sometimes bipartisan or multi-partisan, to carry out privacy oversight of the central bank.

This idea will surely incur criticism because it might introduce another form of constraint of central bank independence. However, this is probably refutable considering the actual practice of central bank independence. Central bank independence can mean personnel independence, tenure protection of the governors, and freedom in exercising monetary policies,[166] but each of these requires congressional support in the first place. In other words, congressional intervention is already inherent in the concept of central bank independence.[167] Admittedly, what we propose in this paper is an *ex-post* and continuous oversight of the central bank by Congress, which is different from the *ex-ante* appointment or authorization of the central bank leadership and fiscal resources as adopted in the current practice.[168] Nevertheless, as long as we limit the scope of this proposed congressional oversight to specific privacy matters, it does not necessarily interfere with the core functions of a central bank.

Specifically, we propose that Congress establish a permanent CBDC privacy safeguard committee that requires the central bank to conduct regular CBDC-related privacy impact assessments. Moreover, the central bank shall report complaints from CBDC users regularly. Sovereigns subject to GDPR may have already had similar designs or requirements.[169] That said, other sovereigns may consider introducing similar mechanisms to safeguard their citizens' privacy orderly. Therefore, we believe this proposed solution remains relevant.

This *ex-post* congressional oversight should compel a central bank to obtain the skills to manage the privacy risk accompanied by CBDC's issuance and circulation. After all, a central bank and other governmental agencies are incentivized to withhold CBDC data for privacy concerns. Effective congressional oversight may require a central bank to credibly

---

[166] Cukierman et al., *supra* note 90; Ana Carolina Garriga, *Central Bank Independence in the World: A New Data Set*, 42 INT L INTERACTIONS 849 (2016).

[167] Courts may also intervene. *See* Cristina Bodea & Ana Carolina Garriga, *Central Bank Independence in Latin America: Politicization and De-Delegation*, 36 GOVERNANCE 59, 71 (2023).

[168] *See* Nicolò Fraccaroli et al., *Central Banks in Parliaments: A Text Analysis of the Parliamentary Hearings of the Bank of England, the European Central Bank and the Federal Reserve* (European Central Bank Working Paper, No. 2442, 2020). *See also* Laurenz Ennser-Jedenastik, *Party Politics and the Survival of Central Bank Governors*, 53 EUROPEAN JOURNAL OF POLITICAL RESEARCH 500 (2014).

[169] GDPR mandates states to conduct privacy impact assessments. *See* Bart Custers et al., *A Comparison of Data Protection Legislation and Policies Across the EU*, 34 COMPUT. L. & SEC. REV. 234 (2018).

commit itself to monitoring by the legislature .

On the other hand, we expect that this congressional oversight might create room for a political struggle between the ruling and the opposing party, where the incumbents would always defend or cover the wrongdoing of the central bank. It is, therefore, essential to demand more transparency on the operational procedures of CBDCs. This can be achieved in the following two ways:

The first is voluntary disclosure. A central bank may establish internal rules to monitor and manage the preservation and access to CBDC data. These rules should be clear to the general public. It should also make regular reports to the multi-partisan committee, as proposed above. The committee would then provide an assessment of the privacy protection performance of the central bank.

Second, the legislative committee may be vested with the power to initiate investigations. Unlike regular assessments, these investigations shall target specific events or misconduct. Therefore, this committee may initiate investigations only when there are sufficient suspicions of privacy infringement. The scope of the investigation may include not only the internal operation of a central bank but also its external relations with outside partnering institutions. The committee may also give recommendations on the internal governance of a central bank.

To enforce this idea, we believe that the legislative committee shall have the authority to discipline the central bank governors for dereliction. This may involve the judicial branch, but the legislature will be responsible for revealing the mismanagement of the central bank. The main objective of these measures is to hold a central bank accountable even if it outsources technical details to other partnering intermediaries.

2. Special Independent Privacy Supervisor

The second option is to legislatively establish a special independent privacy supervisor to oversee the central bank.[170] This idea is similar to the

[170] The Privacy and Civil Liberties Oversight Board ("PCLOB") is arguably the agency closest to our special independent privacy supervisor idea. The PCLOB is an independent agency within the Executive Branch established by the 9/11 Commission Act of 2007. 42 U.S.C § 2000ee. Its mission is to "ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties." PCLOB is mandated with oversight and advisory functions, notably, the power to review the implementation of Executive Branch policies, procedures, regulations, and information-sharing practices related to terrorism prevention to protect privacy and civil liberties. To carry out its mission, PCLOB may access all relevant executive agency records, reports, audits, reviews, documents, papers, recommendations, and any other relevant materials, including classified information. , *History and Mission*, THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/About/HistoryMission (last visited June 16, 2023). Recently, in the Executive Order signed by President Biden to address the GDPR adequacy issue, the PCLOB was authorized to review the Intelligence Community policies and procedures. *Fact Sheet: President Biden Signs Executive Order to Implement the*

data supervisory authority prescribed by GDPR. According to GDPR, a member state needs to establish a supervisory authority to monitor GDPR applications and protect fundamental privacy rights.[171] The nature of such an authority is quasi-judicial and performs primarily enforcement functions.[172] It comprises members with the experience and qualifications necessary to protect personal data and, therefore, should possess sufficient representation and democratic legitimacy.[173] That said, as mentioned previously, GDPR does not apply to all CBDC-issuing sovereigns. Non-EU sovereigns may follow similar standards, but their implementation remains problematic if there lacks a clear legal mandate to support the efforts.

We propose that this independent privacy supervisor may consist of consumer representatives, banking associations, experts on IT and cybersecurity, and human rights activists. Specifically, with the participation of human rights activists, this supervisor will likely pay closer attention to the suspicious misuse of personal data by the issuing central bank. Finally, similar to the previous proposal, this proposal also requires the legislature to take action.

This proposed independent privacy supervisor, mandated by law and the legislature, may supervise a central bank's processing of CBDC data and its data governance regime. It can be further designed as an independent institution that oversees all data governance issues concerning any governmental agencies. In the age of big data and digital transformation, data governance in the public sector has become more pressing and vital.[174] Nevertheless, unlike private enterprises generally disciplined by a sovereign's privacy laws, governmental agencies often fall off the radar.[175] Introducing a dedicated independent privacy supervisor that supervises governmental agencies can fill that gap.

Foreseeably, some might criticize this proposal that the existing privacy supervisor may well undertake the task of overseeing the central bank. Our counterargument is that, to the extent that these privacy supervisors are not independent, it is unrealistic to expect them to adequately supervise other governmental agencies because they may share the same political will with these agencies to be supervised. To ensure its

---

European Union-U.S. Data Privacy Framework, THE WHITE HOUSE (Oct. 7, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

[171] GDPR, *supra* note 118. *See also* SHARMA, *supra* note 119119, at 241.

[172] SHARMA, *supra* note 119, at 246-49.

[173] *Id.* at 242.

[174] *See generally* W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485 (2019).

[175] For instance, as mentioned above, the famous CCPA and CPRA, considered as the most comprehensive privacy regulations in the United States, only apply to "businesses" and therefore do not extend to governmental authorities. CPPA, *supra* note 135.

independence, this independent privacy supervisor should also have sufficient staff with adequate expertise, particularly in data security and privacy protection. To ensure independence, the staff shall further enjoy tenure protection to prevent political interference.

In the meantime, we do not want to exaggerate the advantages of independent privacy supervisors. The common problem of an independent supervisory regime is an insufficient authorization. In some cases, the legislature mandates the independent institution to supervise but retains the power of making a final assessment, rendering the institution simply an investigatory agency.[176] In other cases, the legislature may also weaken the institution's independence by blocking the nomination of its executive members. These moves often result from the political competition between the ruling and opposition parties within the legislature.

On the other hand, there is also a problem with who watches the watchdog. An overpowered independent privacy supervisor may impede the central bank's governance of CBDC and thus infringe on central bank independence. It might further bring stability risk to the financial market if it intervenes excessively in the CBDC's operation.

Therefore, we propose it is necessary to design mechanisms that allow the central bank to appeal to a third party its disputes with this independent privacy supervisor. This prevents the independent supervisor from abusing its power. The third-party needs authorization to mediate between a central bank and its supervisor. Given the potential bias of the legislative branch, the judicial branch is a better candidate to coordinate and even settle the dispute between a central bank and its supervisory institution. The judicial branch often coordinates disputes between the executive and legislative branches. It also helps clarify laws and regulations to disputants. The intervention of a judicial branch does not necessarily settle the dispute, but it provides a solution to prevent the deadlock.

3. Tailor-Made Privacy Protection Regime

Last but not least, we propose a special privacy protection regime tailor-made for CBDCs. A sovereign's privacy protection regime is the frontline defense for addressing CBDC's privacy concerns. Most sovereigns have their privacy laws. Some are aligned with generally accepted global standards, such as the GDPR in the European Union. In contrast, other sovereigns impose their privacy laws and give certain leeway to governmental agencies.[177]

---

[176] The lack of effective supervisory authority often takes place in international cooperation. *See* Eric J. Pan, *Challenge of International Cooperation and Institutional Design in Financial Supervision: Beyond Transgovernmental Networks*, 11 CHI. J. INT'L L. 243 (2010).

[177] For comparative studies of different privacy protection regimes, *see, e.g.,* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115

Although these privacy laws aim to protect a sovereign's citizens from the misuse of their personal data by both the private and public sectors, they generally provide some exceptions or safe harbors for the government when the government processes the data for purposes related to the advancement of public interests, such as criminal detection or investigations.[178] These "public sector waivers" will, to some extent, relieve central banks from the purview of domestic privacy laws and thus aggravate CBDC's privacy concerns. Moreover, as mentioned above, some sovereigns' privacy laws are even inapplicable to governmental agencies.[179]

As a result, we propose rethinking privacy laws' application to government agencies. Specifically, suppose overhauling a sovereign's privacy laws is less politically feasible. In that case, we advocate that it may take a step back and introduce an enhanced privacy protection regime tailor-made for CBDCs, including the CBDC-issuing central bank and related governmental authorities. Again, there are a couple of possibilities.

First, as elaborated above, a government may consider adopting intermediated CBDCs, which disallows a central bank to access retail CBDC information (e.g., payer, payee, the purpose of payments, purchasing items, etc.) and preserve the information only at partnering intermediaries. Under such a design, the issuing central bank will only obtain the wholesale data as it did under the traditional central bank money and commercial bank money division. The retail CBDC data thus remains anonymous on the side of the central bank. Such design will cast most privacy protection duties on the private sector (i.e., the partnering intermediaries). To that extent, the privacy protection regime for CBDC may focus on the private sector, which resembles the privacy protection practice in most sovereigns. It should pay particular attention to the circulation of retail CBDC data from partnering intermediaries to the central bank or other governmental authorities to ensure that the intermediated CBDCs are functioning as committed. This approach arguably better protects citizens' privacy because the private sector is less capable of capturing the privacy supervisors and thus are more likely to comply with privacy protection requirements.

Second, in cases where a sovereign adopts hybrid CBDCs or the variant of one-tier CBDCs, its central bank would possess retail CBDC data and collect and process it for specific legitimate purposes. In that case, it would be difficult to draw a fine line between misuse and legitimate use of CBDC data. To prevent misuse, a privacy protection regime tailor-made for CBDCs can require the central bank to publish or submit privacy

(2017); Douglas W. Arner et al., *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L.J. 623 (2022); Henry Gao, *Data Regulation with Chinese Characteristics, in* BIG DATA AND GLOBAL TRADE LAW 245 (Mira Burri ed., 2021).

[178] SHARMA, *supra* note 119, at 291-294.

[179] Sometimes the application of these rules is unclear, too. *See* Teresa Quintel, *Data Protection Rules Applicable to Financial Intelligence Units: Still No Clarity in Sight*, 23 ERA FORUM 53 (2022).

assessments and board minutes to justify their compliance with related privacy laws, such as the data collection minimization principle and the purpose specification principle. A central bank shall further disclose its cooperation with other governmental agencies, such as law enforcement, to ensure the legitimate use of data. It is also crucial that the central bank has a comprehensive data governance mechanism to help follow privacy protection principles. Most importantly, this mechanism may allow citizens and the legislative branch to oversee the central bank's use of personal data routinely.

Finally, clear legal mandates and strong political determination are always required to ensure compliance with privacy laws on the side of governmental agencies.[180] It is not unprecedented for a privacy supervisor to take disciplinary actions against governmental agencies. A recent example is the Swedish Data Protection Authority, which imposed a fine of 200,000 Swedish kronor on the National Government Service Centre for failing to notify the Data Protection Authority and affected parties about a personal data breach in due time.[181] Whether a privacy supervisor will take similar actions to discipline the misuse of CBDC data or the noncompliance of privacy laws on central banks or other government agencies remains to be observed. However, with the suitable institutional designs, we are optimistic about the disciplinary viability of an independent privacy supervisor to oversee CBDC-issuing central banks.

4. Summary

In this section, we revisit various mechanisms potentially adopted by the government to eliminate or mitigate CBDCs' privacy concerns, including abiding by the existing privacy laws, anonymizing CBDC data (which is arguably less feasible), token-based CBDCs, and intermediated CBDCs. We further demystify some arguably promising designs, such as token-based CBDCs and intermediated CBDCs. We highlight that having a credible mechanism that balances privacy protection, other policy objectives, and central bank independence is the key. We finally propose three potential credible designs, including an ex-post congressional oversight, a special independent supervisory institution, and a tailor-made privacy protection regime. In sum, we argue that there are ways to mitigate

[180] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1737 (2020) (highlighting that "regulators must have broad grants of authority, including rulemaking provisions where necessary, robust civil penalty authority, and the ability to seek injunctions quickly to stop illegal practices" and "without ….. a strong political mandate for enforcement, any privacy framework will merely be a pretext for exploitation").

[181] Press Release, European Data Protection Board, *The Swedish Data Protection Authority Issues Fine Against the National Government Service Centre*, https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-issues-fine-against-national-government_en.

CBDCs' privacy concerns, but a credible disciplinary mechanism is needed to enforce them.

IV. DISCIPLINING CBDC'S PRIVACY CONCERNS FROM AN INTERNATIONAL PERSPECTIVE

All the preceding analyses focus on the domestic context and attempt to establish a domestic legal framework for addressing CBDC's privacy concerns. However, these domestic institutions inevitably risk failure. For one thing, building these domestic institutions requires legislative actions, but many sovereigns may lack the political will to prioritize citizens' privacy concerns over other potential utilities of CBDC. Even if a sovereign finally passes the laws to introduce these domestic institutions, their implementation and enforcement remain questionable.

Fortunate or not, CBDCs' privacy implications do not necessarily restrict to the issuing jurisdiction. After all, CBDC data is essentially electronic records that can cross borders and impact its users regardless of nationality.[182] Therefore, the circulation of a cross-border CBDC allows the issuing central bank to collect, administer, and process CBDC data involving citizens of the receiving sovereigns.[183] This development, in turn, introduces the receiving sovereigns into the landscape.

Receiving sovereigns may be deeply concerned that the issuing sovereign may abuse their citizens' privacy and have legitimate grounds to intervene.[184] More complicated, each sovereign may have different privacy laws and enforcement mechanisms. Therefore, when an issuing sovereign perceives its central bank's use of CBDC data as legitimate, the receiving sovereigns might disagree.[185] To the extent that the receiving sovereigns may extend their privacy laws to the issuing central bank, the cross-border nature of CBDCs brings in an additional gatekeeper of CBDCs' privacy concerns. Furthermore, this gatekeeper may be more credible considering that the privacy supervisors of receiving sovereigns are generally independent of the central bank and other governmental authorities of the

[182] This is particularly likely considering that most sovereigns do not pose restrictions on the use of foreign currency in their domestic jurisdictions. Raphael Auer et al., *CBDCs Beyond Borders: Results from a Survey of Central Banks* 10 (Bank for Int'l Settlements Paper, No. 116, 2021).

[183] To be sure, a central bank may adopt certain technological designs, such as an ID verification scheme, to limit foreigners from using their CBDCs if they consider the cross-border circulation of their CBDCs is unnecessary. BIS 2021 ANNUAL REPORT, *supra* note 36, at 86-87.

[184] The Treasury of the United States, for instance, has expressed its position that "the United States has an interest in ensuring that such systems are aligned with the principles of privacy, human rights, and other democratic values." TREASURY 2022 REPORT, *supra* note 13, at 36.

[185] Such a dispute is particularly likely to occur when the issuing government uses the CBDC data to serve its domestic policy, such as investigating illicit financial activities or controlling capital flow.

issuing sovereign.

In this section, we highlight the possible role of these foreign institutions in disciplining CBDCs' privacy concerns. Specifically, as CBDC evolves into a cross-border payment instrument, it may introduce spillover effects[186] and even infringe on citizens' privacy in receiving sovereigns. We will illustrate how the privacy laws of receiving sovereigns may impose extraterritorial restrictions on the issuing sovereign's CBDC and the potential impact on CBDCs' ongoing development.

A. The Brussels Effect of Modern Privacy Laws and Their Extraterritorial Effect on CBDCs

Our analyses by far establish that to issue CBDC, a central bank might undertake significant compliance costs to comply with its privacy laws. That said, some might argue that these analyses only apply to those sovereigns that take privacy protection into due account. Admittedly, the intensity of privacy protection is different among all sovereigns. As elaborated in the previous sections, we also admit that establishing a robust domestic mechanism for addressing CBDCs' privacy concerns is not an easy task. Therefore, we do not deny that some issuing central banks might face less intensive privacy protection requirements and thus undertake little privacy protection cost.

That said, modern privacy laws bear an extraterritorial character and thus have the potential to extend to foreign central banks. GDPR, for instance, is a notable example that extends beyond the EU's territory and disciplines many non-EU-based enterprises on a unilateral basis. Despite the controversy of this well-known "Brussels Effect,"[187] it serves as a separate disciplinary mechanism highly independent of domestic privacy supervisors and thus introduces additional disciplinary effect. Therefore, even if a central bank is subject to minimal privacy protection requirements domestically, other sovereigns that receive its CBDC might impose more intensive privacy disciplines. This is particularly a concern for those central banks that issue CBDCs as part of their currency internationalization plan.

The extraterritorial character of modern privacy laws finds its justification in this digital era. Thanks to the advancement of communication technology, one can quickly transfer data across the border. The data so transferred thus falls within the possession of foreign data controllers, especially those BigTech giants like the F-A-A-N-G (i.e., Facebook, Amazon, Apple, Netflix, and Google) in the United States or the

---

[186] For CBDCs' potential spillover effect, *see* Cheng-Yun Tsang & Ping-Kuei Chen, *Policy Responses to Cross-Border Central Bank Digital Currencies—Assessing the Transborder Effects of Digital Yuan*, 17 CAP. MKTS. L.J. 237 (2022).

[187] *See generally* BRADFORD, *supra* note 40. *See also* Arner et al., *supra* note 177. For a study on GDPR's Brussels Effect on the United States, *see* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 387-411 (2019).

B-A-T (i.e., Baidu, Alibaba, and Tencent) in China. To protect the privacy of their citizens, many sovereigns have little choice but to design their privacy laws in a manner that extends beyond their domestic territories. This is particularly the case for those sovereigns that witness a significant "export surplus" in data.[188]

GDPR, for instance, applies to "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union," subject to certain limitations.[189] Based on this mandate, GDPR can extend to data controllers outside the European Union, provided that the conditions are met. In light of this possibility, CBDC issued in a sovereign with less rigorous privacy laws is not necessarily immune from GDPR's disciplines.

GDPR's Brussels Effect does not stop here. It further incorporates limitations on cross-border data transfer to sovereigns not subject to GDPR. Specifically, for a data controller to transfer personal data from the European Union to a third country or international organization to which the GDPR is inapplicable, such transfer is prohibited in principle.[190] Exceptional cases include transfers based on the European Commission's ("EC") adequacy decision of the third country's or international organization's level of protection,[191] transfers subject to appropriate safeguards,[192] and other exceptional circumstances.[193] Therefore, even if an issuing central bank is free of GDPR's direct applications, it then faces the challenge of transferring the CBDC data outside the European Union. To make it, it should either adopt appropriate safeguards approved by EC or have its government obtain EC's adequacy decision.[194] In other words, either the central bank's overall privacy protection mechanisms or the issuing sovereign's overall privacy protection laws are subject to EC's assessment.

Moreover, privacy laws in some sovereigns apply to public authorities. GDPR, for instance, makes it clear that the data controller subject to its

---

[188] For instance, some commentators questioned that EU's GDPR is a protectionist economic tool against the United States' and China's technological supremacy. *See* Matthew R. A. Heiman, *The GDPR and the Consequences of Big Regulation*, 47 PEPP. L. REV. 945, 952-53 (2020).

[189] GDPR, *supra* note 118 art. 3.2. The limitations require processing activities to be related to (i) the offering of goods or services to such data subjects in the Union, or (ii) the monitoring of their behavior as far as their behavior takes place within the Union.

[190] *Id.* art. 44(1); Recital 101.

[191] *Id.* art. 45(1).

[192] Such as approved standard data protection clauses, code of conduct, or certification mechanism. *Id.* art. 46(2).

[193] Such as explicit informed consent, specified necessary circumstances, public register, etc. *Id.* art. 49(1).

[194] For a study on how the European Union negotiates with other sovereigns, especially Japan and the United States, on adequacy decisions, *see* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 783-803 (2019).

requirements includes the "natural or legal person, *public authority, agency or other body* [emphasis added]."[195] The Swedish Data Protection Authority's disciplinary action against Sweden's National Government Service Centre in 2020, as mentioned above, is also a real example. Therefore, even if an issuing central bank might claim state immunity to escape the disciplines from domestic privacy laws in its jurisdiction, it remains subject to privacy disciplines in other jurisdictions.

Admittedly, some existing international institutions might preclude the extraterritorial application of privacy laws to foreign central banks. For instance, some privacy supervisors might refrain from adopting disciplinary actions against foreign central banks out of international comity. That said, to the extent that most central banks prefer adopting two-tier CBDCs and thus invite private partnering intermediaries to act on their behalf, privacy supervisors of receiving sovereigns may instead enforce privacy laws against these intermediaries. For instance, instead of fining the issuing central bank, they may suspend the CBDC-related business of the partnering intermediaries operating in their territories. This indirect disciplinary effect can still impact the issuing central bank.

The long controversy between the European Union and the United States over the transatlantic cross-border data flow well illustrates this possibility.[196] The controversy concerns data transfer from the European Union to the United States. EC released the adequacy decisions of the United States' level of privacy protection based on the Safe Harbor Privacy Principles in 2010 and the EU-U.S. Privacy Shield Framework in 2016. However, in *Schrems I* in 2015[197] and *Schrems II* in 2020,[198] the European Court of Justice ("ECJ") twice overruled the adequacy decision based on the finding that the United States' privacy protection is limited "to the extent necessary to meet national security, public interest, or law enforcement requirements."[199] The ECJ was particularly concerned about Section 702 of the United States Foreign Intelligence Surveillance Act, which "does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by

[195] GDPR, *supra* note 118 art. 4.7.

[196] For literature summarizing the transatlantic data flow controversy, *see, e.g.,* W. Gregory Voss, *Transatlantic Data Transfer Compliance*, 28 B.U. J. SCI. & TECH. L. 158 (2022); Ira Rubinstein & Peter Margulies, *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground*, 54 CONN. L. REV. 391 (2022).

[197] Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).

[198] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, ECLI:EU:C:2020:559 (July 16, 2020).

[199] *Id.* ¶ 164.

those programmes."[200] ECJ's Decision forced President Biden of the United States to sign an executive order to enhance the privacy protection of the United States' signals intelligence activities to regain EC's adequacy decision,[201] which is now under EC's contemplation.[202]

Notably, the above controversy did not arise from EC's disciplinary action against any intelligence authorities in the United States. Instead, it stemmed from the filing by an Austrian citizen, i.e., Schrems, against Facebook's data transfer to the United States.[203] However, because Facebook conducts the transatlantic data transfer based on the EC's adequacy decision of the United States' level of privacy protection, the United States is forced to enhance its privacy protection level to facilitate the transatlantic data transfer. Similarly, a receiving sovereign may force a CBDC-issuing sovereign to improve its privacy protection level by adopting disciplinary actions against the cross-border transfer of CBDC data by private partnering intermediaries.

B. The International Gaming Perspective of the Brussels Effect on CBDC

To apply a sovereign's privacy laws extraterritorially to the central bank of another sovereign, the issuing central bank must be at least involved in collecting or processing the CBDC data of the receiving sovereigns' citizens. This is a crucial connecting factor, which establishes a genuine concern of the receiving privacy supervisors that the issuing central bank and its partnering intermediaries might misuse the CBDC data of its citizens.

To control the above legal risk, an issuing central bank may issue CBDC only to its citizens as a response. Choosing this approach, however, necessarily discourages itsCBDC from evolving into a cross-border payment instrument. Moreover, the central bank cannot reap the currency internationalization benefit of CBDCs. If internationalizing its currency remains on the agenda of the issuing central bank, it should address the privacy concerns of its CBDC in receiving sovereigns even if its domestic laws do not require so.

Based on this observation, we wish to raise an international gaming perspective on CBDCs' privacy concerns. The preceding analyses have established that the Brussels Effect of modern privacy laws may serve as a practicable tool to inhibit the development of foreign CBDCs. In this global CBDC competition, some sovereigns have taken the lead while others

---

[200] *Id.* ¶ 180.

[201] Enhancing Safeguards for United States Signals Intelligence Activities, Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 7, 2022).

[202] *Questions & Answers: EU-U.S. Data Privacy Framework, Draft Adequacy Decision*, EUROPEAN COMMISSION (Dec. 13, 2022), https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632.

[203] *See supra* notes 197and 198.

remain lagging. The follower sovereigns, however, may use their privacy laws as a weapon to preclude other developed CBDCs from evolving into cross-border payment instruments. At the minimum, they may prevent other developed CBDCs from entering their domestic markets and thus preserve the space for developing their native CBDCs.[204]

Then what would the world be if most major sovereigns exerted this Brussels Effect and extended their privacy laws to CBDCs of other sovereigns? If this move becomes common practice among world privacy supervisors and thus ousts foreign CBDCs from their domestic markets, it would create a silo effect on CBDCs. Each CBDC system would become isolated islets that only serve their domestic markets. In the end, no CBDC could evolve into a globally-accepted cross-border payment instrument.[205]

The direct beneficiary of this unintended development would be the existing cross-border payment system. As inhibited by worldwide privacy laws, CBDCs would become less of a threat. Potential beneficiaries include emerging cross-border payment instruments. Global stablecoins, for instance, might have some edge,[206] particularly if the issuer volunteers to undertake the compliance cost, including those arising from financial supervision and privacy protection requirements.[207]

C. Harmonizing Cross-Border Privacy Laws and the Central Bank Independence

Is the triumph of private payment instruments, such as stablecoins, a happy ending? We are skeptical. Should major sovereigns desire not to position their CBDCs as local payment instruments, they should figure out ways the Brussels Effect stemming from existing privacy protection laws.

---

[204] To be sure, some studies disagree that CBDC may escalate a sovereign's currency to a dominant global currency. BIS, for instance, highlighted that the cross-border use of CBDCs requires international cooperation, which thus permits sovereigns various measures at hand to limit the circulation of foreign CBDCs in their territories. BIS 2021 ANNUAL REPORT, *supra* note 36, at 86-87. The Treasury of the United States also held an optimistic view that "the prominence of the dollar reflects factors beyond payment system efficiency. These factors include the United States' strong economic performance; sound macroeconomic policies and institutions; open, deep, and liquid financial markets; institutional transparency; commitment to a free-floating currency; and strong and predictable legal systems. In the near term, foreign CBDCs and private digital assets by themselves likely offer little new competition to the dollar beyond traditional foreign fiat currency, particularly because they do not address the structural factors above." TREASURY 2022 REPORT, *supra* note 13, at 34.

[205] A similar observation argues that an overuse of the extraterritorial application of privacy laws among major economies might lead to the end of the Internet as a global commons. Arner et al., *supra* note 18, at 47–53.

[206] The Federal Reserve and the Treasury, for instance, have noticed the potential of stablecoins to evolve into a more promising payment instrument. FEDERAL RESERVE 2022 REPORT, *supra* note 11, at 11-12; TREASURY 2022 REPORT, *supra* note 13, at 17.

[207] For the potential regulation of stablecoins, *see* PRESIDENT'S WORKING GROUP ON FINANCIAL MARKETS ET AL., REPORT ON STABLECOINS 15-21 (2021).

The said Brussels Effect results from the unilateral yet extraterritorial application of laws. Therefore, major sovereigns may start by exploring bilateral, plurilateral, or even multilateral dialogues to harmonize the impact of domestic privacy laws.[208] In world trade practice, sovereigns have already begun to explore ways to harmonize cross-border privacy laws through initiatives or forums, digital trade chapters in free trade agreements, digital economy agreements, etc.[209]

Nevertheless, the progress of privacy law harmonization remains limited. For instance, in the United States-Mexico-Canada Agreement ("USMCA"), the three countries agreed on a provision "[r]ecognizing that the Parties may take different legal approaches to protect personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes."[210] However, they merely promise to "*endeavor to* exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them."[211]

Similarly, on cross-border data transfer, although the USMCA obliges each country not to prohibit or restrict the cross-border transfer of information,[212] it contains a broad exception if the prohibition or restriction is "necessary to achieve a legitimate public policy objective," subject to the specified conditions.[213] Other international economic agreements, such as CPTPP and DEPA, exhibit similar narratives.[214] While major sovereigns have recognized the importance of harmonization of cross-border data flow and privacy law, they fail to take a step further.[215]

Against the existing privacy law harmonization initiatives, we wish to note the associated central bank independence concern. While sovereigns

---

[208] For a discussion of the different approaches to establish cross-border privacy cooperation, *see* Arner et al., *supra* note 18, at 57-65.

[209] For a discussion of the potential driving force and resistance of these cross-border privacy arrangements, *see, e.g.,* Schwartz & Peifer, *supra* note 177.

[210] United States-Mexico-Canada Agreement art. 19.8(6), July 1, 2020.

[211] *Id.* (emphasis added)

[212] *Id.* art. 19.11(1) ("No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.").

[213] *Id.* art. 19.11(2) ("provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.").

[214] For instance, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP") and Digital Economy Partnership Agreement ("DEPA") contain similar provisions. *See* CPTPP, *supra* note 43 arts. 14.8(5), 14.11; DEPA, *supra* note 43 arts. 4.2(6), 4.3.

[215] For a discussion of the obstacles to the transatlantic privacy law harmonization, *see generally* W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405 (2019).

have started to explore methods[216] to harmonize their privacy laws, they explore them mainly through trade or economic agreements, such as USMCA, CPTPP, or DEPA. This means that a sovereign's trade negotiation agency is typically in the taking charge of negotiation, which risks marginalizing the central bank. The central bank will likely need the trade negotiation agency's assistance to reach some progress on the privacy law harmonization related to CBDC. This operation inevitably allows the executive and legislative branches to interfere with the central bank's operation.

V. CONCLUSION

In the coming years, CBDCs may innovate payment systems, reduce frictions of cross-border money transferring, enhance social welfare, and empower central banks. Nevertheless, these aspirations come with costs and problems. Many regulatory issues need to be addressed, particularly privacy protection. As most people would readily appreciate, unlike cash, digital cash like CBDCs can track trails of citizens' transactions and, therefore, may infringe on citizens' privacy. The issuing central bank might sometimes be required by its government or other agencies to share CBDC data, which subjects citizens' privacy to significant risks. Some disciplinary safeguards must be in place to prevent that from happening, but the unsettled problem is how to design these safeguards without jeopardizing central bank independence.

This paper argues that there are three potential designs to credibly address privacy concerns of CBDCs in a domestic context, including an ex-post congressional oversight, a special independent supervisory institution, and a tailor-made data protection regime. We also recognize that building these domestic regimes requires legislative action. Still, many sovereigns may lack the political will to prioritize citizens' privacy concerns over other potential utilities of CBDCs. Therefore, this paper also explores the possible role of the foreign legal framework and international regime in disciplining regulating issuing central banks and their governments under modern privacy protection laws. Notably, the so-called Brussels Effect, resulting in the unilateral and extraterritorial application of privacy laws, may play some role in disciplining issuing central banks. We anticipate that major sovereigns may start by exploring bilateral, plurilateral, or even multilateral dialogues to harmonize the impact. Applying modern privacy laws and proper supporting mechanisms may serve as effective disciplines on CBDCs and their issuing central banks.

---

[216] These methods may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement; broader international frameworks; appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or other avenues of transfer of personal information between the Parties. *See* DEPA, *supra* note 43 art. 4.2(6).