Disciplining Central Banks: Addressing the Privacy Concerns of CBDCs and Central Bank Independence

Cheng-Yun Tsang[a], Yueh-Ping (Alex) Yang[b] and Ping-Kuei Chen[c]

Paper prepared for 2022 DC Fintech Week submission

Abstract

Central bank digital currency ("CBDC") is a crucial FinTech development that aspires to renovate the current payment system. After the COVID-19 pandemic hit the world, CBDCs' promises to reduce personal contact, facilitate socially desirable use of money, and initiate more targeted monetary measures increased their popularity. In addition, CBDCs can potentially serve as a tool to internationalize a sovereign's currency. As world central banks have gradually formulated the consensus in structuring CBDCs, the regulatory aspects of CBDCs deserve more attention. Among the regulatory issues related to CBDCs, observers often mentioned their association with privacy concerns, but comprehensive studies on this aspect remain limited.

This paper discusses the privacy concerns associated with CBDCs and attempts to introduce disciplines upon CBDCs and their issuing central banks. We firstly demonstrate the privacy implications of CBDCs and highlight the risks that sovereigns might misuse CBDCs to serve their agendas. We then discuss, in a domestic context, several institutional designs that may address privacy concerns and propose several disciplinary mechanisms that may enforce the privacy protection laws against issuing central banks. We finally highlight the extraterritorial character of modern privacy laws, which creates room for foreign privacy protection regulators to discipline the CBDCs of other jurisdictions. Through these analyses, we argue that the application of modern privacy laws and proper supporting mechanisms may effectively discipline CBDCs and their issuing central banks.

Keywords: CBDC, privacy protection, privacy law, extraterritoriality, programmable money, Brussel Effect

[a] Associate Professor, College of Law, National Chengchi University (NCCU); Director of the Financial Innovation and Technological Evolution Center (FINTEC) at NCCU Law; Visiting Scholar, Duke University School of Law (2020); Visiting Fellow, UNSW Law and Justice (2020-2023); 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) Research Project Grant "Constructing A Cross-Border-and-Industry Regulatory Framework for Interactions between Financial Systems and Technological Innovations" (MOST 110-2636-H-004-003 -). The author can be reached at cytsang@nccu.edu.tw

[b] 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). This paper is funded by the National Science and Technology Council of Taiwan (R.O.C) Emerging Young Scholars Research Project Grant (MOST 111-2628-H-002-002). The author can be reached at alexypyang@ntu.edu.tw

[c] Associate Professor, Department of Diplomacy, National Chengchi University (NCCU). University of Maryland Ph.D. at Government and Politics. The author can be reached at pkchen@nccu.edu.tw

Introduction

Central banks worldwide have started to devote resources in studying and developing their central bank digital currency, or CBDC.[1] The motives for a central bank to issue CBDC may include many facets, ranging from saving the money-printing cost, combatting counterfeit money, ensuring citizens' access to the payment system, transparentizing the money flow, and facilitating the clearing and settlement of payments. After the outbreak of the COVID-19 pandemic, CBDC has received even more attention. For instance, CBDC may facilitate remote transactions and thus help reduce personal contact and the spread of the virus. CBDC may also enable a more targeted implementation of the bailout and monetary policies and thus help stimulate the economy slowed down by the pandemic.[2] CBDC's impact at the international level is also significant. CBDCs facilitate cross-border transactions by speedy and secure clearing.

However, the issuance and administration of CBDC might impose additional regulatory obligations upon central banks. This paper will focus on a specific regulatory area related to CBDC, i.e., privacy regulations. Commentators have noticed the potential privacy concerns associated with CBDC. In a nutshell, through the CBDC's ledger, central banks may observe, monitor, and even control the cash flow of their sovereign currency more efficiently. This enhanced efficiency, however, inevitably triggers societal concern over the financial privacy of general citizens. That said, many contracting considerations, e.g., AML/CFT, may preclude central banks from issuing anonymous CBDC. Balancing the utility of CBDCs against their privacy concerns thus becomes a crucial issue for CBDCs' ongoing development.

The privacy implications of CBDC, as raised above also challenge the central bank independence. Alleviating the public's privacy concerns against CBDC requires some disciplines upon central banks, such as the legal requirements under personal data protection laws. Disciplining central banks, however, risks contradicting the central bank independence. Even if related disciplinary mechanisms are in place, ensuring these mechanisms' credibility is also challenging. For instance, which agency should be charged with the responsibility to enforce these disciplines against central banks? With what kind of regulatory tools? These regulatory issues all call for a sophisticated set of legal designs.

In this paper, we attempt to fill the above void and propose solutions to addressing the privacy concerns of CBDCs. In Part II, we elaborate on the challenges posed by CBDCs to central bank independence and use the privacy concerns of CBDCs to illustrate them. In Part III, we discuss the potential CBDC designs that may 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 and highlight that the Brussels Effect of modern privacy laws may introduce foreign discipline against central banks issuing CBDCs. We conclude this paper in Part V. We anticipate fostering not only the development but also an orderly development, of CBDC.

---

[1] For a comprehensive survey, *see generally* THE BLOCK RESEARCH, A GLOBAL LOOK AT CENTRAL BANK DIGITAL CURRENCIES: FROM ITERATION TO IMPLEMENTATION (2020); COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES ("CPMI"): MARKETS COMMITTEE, CENTRAL BANK DIGITAL CURRENCIES (2018).

[2] 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* (Eur. Banking Inst. Working Paper No. 65, 2020).

I. Privacy Concerns of CBDC and the Challenges of Central Bank Independence

A. CBDC: A New Mandate 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.[3] These mandates gradually erode the independence of central banks as they play a role in the welfare of citizens.[4] So far, these burdens are mostly related to achieving government objectives through macroeconomic management. The complexity of these tasks create numerous partnership between central bankers and their governments. Principal-agent problems become severe and frictions between the two have become more common. President Trump's criticism of Federal Reserve policies, Turkish President Erdogan's expulsion of central bankers[5], and Azerbaijan President Aliyev's dismissal of his central bank governor, who served 27 years, all suggest that government intervention into central banks has been increasingly stringent.[6]

A growing number of countries have been exploring, testing, and developing CBDCs.[7] It is widely believed that the urgency to promote financial inclusion and the need to respond to the rise of private-sector crypto-assets gave such a trend momentum. Shortly, it is very likely to see more countries give life to CBDCs and use them for retail purposes in a scalable manner. By far, the consensus among policymakers seems to be that a CBDC works most properly through a two-tier architecture and should bear no interest. Such design minimize the impact on the role of commercial banks.[8]

---

[3] 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?* (2010), BIS Working Papers No 326, at 22-23, available at https://www.bis.org/publ/work326.pdf (last visited August 23 2022).Adina Criste and Iuila Lupu, *The Central Bank Policy Between the Price Stability Objective and Promoting Financial Stability* (2014), Procedia Economics and Finance, Vol. 8, at 221; Mario I. Blejer, *Central Banks and Price Stability: Is A Single Objective Enough?* (November 1998), Journal of Applied Economics, Vol. I, No. 1, at 105-106; Phillip Harvey, *What is Full Employment-and Why the Definition Matters* (2016), the International Post Keynesian Conference University of Missouri at Kansas City, at ; Sander Oosterloo and Jakob de Haan, *Central banks and financial stability: a survey* (December 2004), Journal of Financial Stability, Volume 1, Issue 2, at 262.

[4] 9. Mervyn King and Dan Katz, Central Banks Are Risking Their Independence (August 23, 2021), Bloomberg, https://www.bloomberg.com/opinion/articles/2021-08-23/central-banks-are-risking-their-independence-mervyn-king-dan-katz; Alex Cukierman, Steven B. Webb, and BilinNeyapti, Measuring the Independence of Central Banks and Its Effect on Policy Outcomes (1992), The World Bank Economic Review, Vol. 6, No. 3.

[5] Sarah Binder and Mark Spindel, Why is Trump attacking the Federal Reserve? We answer your questions, Washington Post, August 27, 2019, https://www.washingtonpost.com/politics/2019/08/27/why-is-trump-attacking-federal-reserve-we-answer-your-questions/ (last visited August 23, 2022).

[6] Den Hardy, Azerbaijan appoints new governor after dismissing predecessor, Central Banking, August 13, 2022, https://www.centralbanking.com/central-banks/governance/7946306/azerbaijan-appoints-new-governor-after-dismissing-predecessor (last visited August 23, 2022)l.

[7] Anneke Kosse and Ilaria Mattei, *Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies* (May 2022), BIS Papers No.125, at 3, available at https://www.bis.org/publ/bppdf/bispap125.pdf (last visited August 23, 2022).

[8] Consensus among the adoption of CBDC, s*ee* BIS, *Central bank digital currencies: foundational principles and core features* (2020), https://www.bis.org/publ/othp33.pdf (last visited August 23, 2022).

CBDCs bring significantly more responsibility to central banks. Central banks have been mandated to develop and facilitate the operation of CBDCs. It includes the design of a secure and reliable CBDC that prevents counterfeit digital money, a fully operational system that maintains and verifies transactions, an electronic payment system that accommodates different payment platforms developed by payment service providers ("PSP"), and a mechanism that effectively enforces AML/CFT regulations.

Building a CBDC system further requires horizontal coordination between different agencies within a government. It would at least bring together the manager of national ID system, financial supervisory agencies, and cybercrime investigation agencies. The two-tier architecture of CBDC also requires commercial banks, Payments Services Providers (PSPs), or Third-Party Service Providers (TSPs) to cooperate with central banks. Such an enormous cooperation project requires central banks to consider how CBDCs can satisfy the mandates of different private and public institutions. The governance of CBDCs inevitably expands the power of central banks. As governments increasingly intervene in central bank independence, the executive branch will likely have more control over CBDCs and the services involving CBDCs.

B. CBDC's Achilles Heel: Privacy Concerns

Issuing CBDCs raises the concern that central banks can observe, monitor, and even control cash flow more effectively. More importantly, central banks may identify users by their transactions and further track and analyze them. Central banks usually do not need user data to achieve their mandates, but other government agencies may find these data very useful. The privacy concern is not only about how central banks manage user information, but also central banks' partnership with other agencies.

1. CBDC and the Inevitable Privacy Implications

CBDC design is highly flexible. Central banks choose their designs to accommodate the need of digitalization and improve financial inclusion. To be sure, allowing effective cash flow tracking is simultaneously a benefit of CBDC. The "programmability" of CBDC suggests that it is technically feasible to limit the amount and locations when people use certain types of money, such as social welfare programs[9]. Therefore, a government may substitute programmed CBDCs for government-issued vouchers designed for specific purposes.[10] For example, a government may issue credits in CBDCs that can only be used to reserve hotels, which is a more efficient tool to stimulate the tourist industry than government-issued vouchers. Central banks can further decide how and where certain CBDCs are applicable by combining government services. They can also allow transactions to fail if there are signs of illicit activities. Central banks will thus have a role in credit and resource redistribution, a task that usually bestows on governments. In practice, it will be the government who provide guidance to central bankers. The government create a list of

[9] For the idea of Programmable Money, Alexander Lee, What is programmable money?, FEDS Notes, June 23, 2021, https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.htm (last visited August 23, 2022).

[10] It is worth considering that there is a distinction between programmable money and programmable payments. CBDC has the potential to enable both. See Jonas Gross, Programmable Money and Programmable Payments, September 29, 2020, https://jonasgross.medium.com/programmable-money-and-programmable-payments-c0f06bbcd569 (last visited August 23, 2022).

services and rules and leave it to the central bankers. Central banks are responsible for setting up the CBDC system to achieve the government's policies.

To achieve the above-contemplated benefits, central banks will require identification during CBDC transactions. CBDC's identification requirement, however, creates privacy concerns that are very different from cash. Cash is anonymous, and there is no record of who owns or transacts the said cash. In contrast, CBDC is different since its ownership and transaction records are kept in certain data servers most likely administered by central banks. Central banks may further decide what kind of information will be preserved, how long it will be preserved, and who can access data under certain circumstances when designing CBDCs.

Moreover, given the concern of AML/CFT and other illegal use of CBDC, it is justified for central banks to retain the ability to trace and monitor transactions.[11] To be sure, if a central bank adopts the two-tier CBDC system, the KYC process will be done by commercial banks or other licensed PSPs. That said, central banks will be responsible for verifying transactions and record keeping. Therefore, the central bank will possess user information and transaction records. Even if central banks commit to dis-identifying user information to keep their commitment to user privacy, this commitment alone could not eliminate the possibility for central banks or other agencies, such as law enforcement and intelligence agencies, to piece up information from other sources.[12]

2. CBDC's Privacy Concerns and Central Bank Independence

To the extent that central banks cannot eliminate the privacy concerns, the next question becomes how to discipline central banks to reduce the privacy concerns to a tolerable level. Disciplining central banks from a privacy protection perspective entails certain legal designs. For instance, under what conditions are central banks permitted or even required to process these records or even share these records with other governmental agencies? How does a central bank ensure that it will follow the data laws, such as the minimization principle? These legal designs intend to discipline central banks, but they may also risk compromising central bank independence.

On the other hand, to gain access to CBDC data to accommodate its interests, other governmental agencies may have increased motivation to interfere with central banks. When a government has such access, there is a risk of privacy infringement and potential human rights violations.[13] Central bank independence against other governmental agencies becomes needed in this scenario.

i. CBDC Data and the Government's Inherent Conflicts of Interest

[11] Daniel Dupuis, Kimberly Gleason, and Zhijie Wang, "Money Laundering in a CBDC World: A Game of Cats and Mice," *Journal of Financial Crime* 29, no. 1 (January 1, 2021): 171–84, https://doi.org/10.1108/JFC-02-2021-0035.
[12] China's digital Yuan is a significant example. The People's Bank of China has access to transaction data even under the so-called "controllable anonymity", see Martin Chorzempa, "Promise and Peril of Digital Money in China Digital Currencies: Risk or Promise?," *Cato Journal* 41, no. 2 (2021): 295–306.
[13] Outlining the issues about using CBDC might introduce privacy concerns, Gabriel Soderberg, etc.; behind *the Scenes of Central Bank Digital Currency Emerging Trends, Insights, and Policy Lessons*, IMF Fintech Note 24-15 (February 2022).

Governments worldwide, democracies and authoritarian states alike, are keen to make public commitments to user privacy. But these commitments are likely to be a cheap talk. There is little, if any, check-and-balance to 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 invading privacy to fulfill their mandates. Law enforcement, crime prevention, intelligence detection, or even national security can benefit from CBDC data. In brief, the government has an inherent conflict of interest.

When a government chooses to initiate such surveillance and employ its central bank to do so, not every central bank can say no. Admittedly, most major central banks enjoy independence, and it has long been a widely-accepted principle. Nonetheless, it is not uncommon to see elected politicians who demand central bank governors follow their agenda. When a government requires its central bank to utilize CBDC data, it poses a severe threat to citizens' privacy and jeopardizes the central bank's independence.

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. They may anticipate violent behavior based on the purchasing records of the protesters. CBDCs provide government agencies with a tool to efficiently complete their tasks. They will have the motivation to utilize this tool if the circumstance permits,[14] including by compromising the central bank independence.

Central banks are not mandated to address national security or enforce AML/CFT. They also do not possess the expertise to facilitate 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 records 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.

ii. Central Banks and the Uneasy Task of Privacy Protection

Even if central banks can manage the above conflicts of interest concern, privacy protection remains a challenging task for central banks. Central banks are not designed to deal with data, not to mention a very sizable one like CBDC data. If a central bank has to store, process, and protect CBDC data, it must implement a well-crafted data governance regime to comply with relevant data protection laws.

Data governance, however, could be beyond the central bank's capacity. Modern data protection laws, such as the General Data Protection Regulation ("GDPR") of the European Union,

[14] *See* The Risks to Society of Central Bank Digital Currencies, Finextra, January 17, 2021, https://www.finextra.com/blogposting/21584/the-risks-to-society-of-central-bank-digital-currencies (last visited August 23, 2022); Sofie Blakstad and Robert Allen, "Central Bank Digital Currencies and Cryptocurrencies," in *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*, ed. Sofie Blakstad and Robert Allen (Cham: Springer International Publishing, 2018), 87–112, https://doi.org/10.1007/978-3-319-76014-8_5.

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.[15] Suppose a central bank or any of its governmental agencies attempt to collect or use available CBDC records to pursue certain public functions. In that case, it will inevitably engage in personal data processing and shall abide by these principles accordingly. Compliance with these regulations, however, is easier said than done.

Taking the principle of lawfulness as an example. If a central bank wishes to use the CBDC data without obtaining the user's consent, modern privacy laws typically require a specific and unambiguous legal mandate that lays down the legal basis for the said data processing.[16] In other words, the central bank may not simply resort to the abstract concept of public goods. In the absence of 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 privacy laws require informed consent, while blanket consent by data subjects to the future processing of their data for open-ended purposes is not qualified.[17] Accordingly, to use the CBDC data, the central bank must possess the legal expertise to obtain qualified informed consent, such as how to specify 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 privacy laws impose many internal control organizations upon data controllers, such as the requirements related to records, security, data breach notification, impact assessment, data protection officer, etc. By withholding the CBDC data, the central bank needs to implement appropriate technical and organizational measures to ensure that their data processing is per the data protection laws.[18] This is a significant change to the central bank practice because central banks that only issue physical cash do not obtain personal data from there 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 significant amount.

In sum, issues surrounding data governance are many folds. All of them require expertise that central banks generally do not have. To make the case even worse, today's central banks suffer from "distraction diseases" in the sense that they are undertaking too many missions ranging from ensuring price stability and full employment to tackling climate change and curing inequality. Given so many agendas on central banks' plates, central banks do not necessarily have extra capacity to ensure data governance to safeguard the CBDC data.

iii. Central Banks and the Uneasy Task of Data Security

To maintain a secure and efficient CBDC service, central banks must step into information technology they are unfamiliar with. Central banks, however, do not necessarily have the technological capacity to issue CBDC. Due to resource and talent constraints, many central banks cannot afford to hire information engineers and data scientists. Therefore, while laws may mandate

[15] GDPR, art. 5(1).
[16] GDPR, art. 6.3.2.
[17] *See* GDPR – Consent, https://gdpr-info.eu/issues/consent/ (last visited Mar. 5, 2021).
[18] GDPR, art. 24.1.1.

central banks to be responsible for maintaining and securing CBDC data, central banks may not have the expertise to tackle the related cyber risk.

Moreover, as the two-tier structure has become mainstream, the issuing central bank will have to cooperate with certain third-party service providers and PSPs. For example, some central banks collaborate with commercial banks to conduct KYC and distribution or engage technology solution providers or TSP to store, process and analyze data. This further complicates the question of data management. A glitch or misstep by these partnering institutions may fare into a cyber security event or privacy infringement. In that case, it would probably be the central bank's responsibility to clean the mess. To prevent the disaster, the issuing central banks need to know how to prevent that from happening and possess the necessary skills to supervise their partnering institutions. Unfortunately, this know-how or skills are typically not within the central bank's capacity scope.

C. Summary

All of the above-mentioned begs a profound question of the long-lasting principle of central bank independence and its viability in the age of rising CBDC adoption. On the one hand, this paper argues that the rise and use of CBDC may erode such independence and turn central banks into rather politically-oriented machines. Specifically, in light of the abundant value of CBDC data, other governmental agencies have all the potential to force central banks to intervene in issues they do not necessarily have the mandate or capacity to tackle. On the other hand, this paper argues that the potential misuse of the CBDC data by central banks warrants some privacy disciplines upon central banks. Imposing these privacy laws upon central banks, however, might also compromise the central bank independence.

Among the growing literature on CBDC, we see a gap in such a discussion and a surprisingly light-touch focus on the grave issue of privacy protection. Therefore, this paper aims to fill this gap and highlights the importance and urgency of rethinking privacy concerns in the context of CBDC issuance and circulation and proposes potential solutions to address these concerns.

II. Disciplining CBDC's Privacy Concerns from A Domestic Perspective

In this section, we specify several CBDC models that may mitigate the privacy concerns of CBDC. On that basis, we further discuss how domestic laws may be designed to address the privacy concerns of CBDC.

A. The Myth of "Token-Based CBDC"

Before further discussion, we wish to demystify the alleged privacy-proof function of the so-called "token-based CBDC." Ordinary CBDC generally adopts the so-called "account-based" design. Under this design, each CBDC holder needs to apply for a CBDC account for conducting CBDC transactions. Through the KYC process for opening a CBDC account, the central bank would further know the identity of each CBDC holder. To the extent that the central bank maintains a CBDC ledger that documents the CBDC transactions of each CBDC holder, it possesses the information of the CBDC stock and transactions of each CBDC holder, which triggers privacy concerns.

To alleviate the privacy concerns, most central banks appear to prefer a hybrid of account-and-token-based design of CBDC, claiming that this design balances traceability and privacy protection.[19] For instance, under some central banks' design, smaller CBDC transactions may be done in the form of token-based CBDC, which permits offline transaction that does not require identification. Many commentators also advocate that a token-based CBDC could significantly address privacy concerns as it functions similarly to digital cash.[20] The offline transaction viability of token-based CBDC further gives users some transactional anonymity.[21]

The privacy-proof function of token-based CBDC, however, is exaggerated. The issuance and circulation of token-based CBDCs still require basic KYC procedures and information, only that the required form of identification is simpler.[22] For example, various CBDC pilot programs require the user's mobile phone numbers. Moreover, after being connected to the web, the records of offline transactions of token-based CBDC will eventually be documented in the central bank's CBDC ledger. In short, CBDC inevitably implicates identification, and token-based CBDC is not free from it.[23]

Some may well argue that as long as this information (e.g., mobile number, email address, etc.) is merely in the hand of the partnering banks or PSPs and does not fall in the hand of the issuing central bank, it is safe to say that these CBDCs will not incur privacy concerns. However, one will hardly imagine that a partnering bank or PSP can really say no to their government should the government present legitimate reasons. If that is the case, there remains a possibility, regardless of how minor that would be, that a government can utilize the KYC and transactional data to monitor CBDC holders if it wants. Such a Levitan-style assumption is not remote, as governments have an abundant history of abusing data.[24]

In sum, this paper argues that privacy concerns, which are the most challenging issue behind the idea of CBDCs, cannot be simply solved by structuring the CBDC as token-based. It begs the fundamental question of a sovereign's power and will. Be it a monarchy or democracy, governments monitor and even try to control citizens to maintain their power and legitimacy.

B. Taking CBDCs' Privacy Concerns Seriously

[19] CBDCs: an opportunity for the monetary system, BIS Annual Economic Report 79 (2021).

[20] *See, e.g.*, Karin Thrasher, *The Privacy Cost of Currency*, 42 MICH. J. INT'L L. 403 (2021). *See also* Christian Grothoff and Thomas Moser, "How to Issue a Privacy-Preserving Central Bank Digital Currency," *SUERF Policy Brief*, no. No 114 (June 2021), https://www.suerf.org/suer-policy-brief/27227/how-to-issue-a-privacy-preserving-central-bank-digital-currency.

[21] Being offline does not mean complete anonymity, see the experiment in Ye Wang et al., "Print Your Own Money: A Cash-Like Experience for Digital Payment Systems," *ArXiv Preprint ArXiv:2104.10480*, 2021. Other claim that full anonymity is technologically feasible, see Jonas Gross et al., "Designing a Central Bank Digital Currency with Support for Cash-Like Privacy," SSRN Scholarly Paper (Rochester, NY, July 22, 2021), https://doi.org/10.2139/ssrn.3891121.

[22] IMF, *supra* note 13, at 10-11 (2022)

[23] For related criticism of token-based CBDC, *see* John Crawford et al., *FedAccounts: Digital Dollars*, 89 GEO. WASH. L. REV. 113, 151-55 (2021).

[24] For arguments and counterarguments of how the world had become am administrative state and whether there is any cure, see Cass R. Sunstein and Adrian Vermeule, LAW & LEVITHAN – REDEEMING THE ADMINISTRATIVE STATE (Harvard University Press 2020); David Ballaschk and Jan Paulick, "The Public, the Private and the Secret: Thoughts on Privacy in Central Bank Digital Currencies," *Journal of Payments Strategy & Systems* 15, no. 3 (September 1, 2021): 277–86.

Below we specify three potential models that central banks may consider adopting for addressing CBDC's privacy concerns.

1. Undertaking the Privacy Protection Duties

The simplest, and perhaps the most common way for central banks to respond to CBDC's privacy concerns is to comply with existing privacy protection laws. Most central banks might choose to undertake the privacy protection obligations imposed by the existing privacy protection laws and introduce necessary protective measures. They might be willing to undertake it, particularly if it assesses that the expected benefit arising from CBDC surpasses the compliance cost.[25]

The concern with this approach is its 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 jurisdictions might even claim the protection of state immunity. These all beg the question of how to establish a credible disciplinary regime against central banks.

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

Some central banks might consider anonymizing the CBDC data to avoid the application of privacy laws. Modern data protection laws do not apply to the processing of anonymous data, that is, personal data that is rendered anonymous in a manner that the data subject is no longer identifiable.[26] If a central bank anonymizes or deidentifies the CBDC data, it no longer holds personal data and may thus be free from data protection duties.

Data anonymization or deidentification, however, is not an easy 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.[27] In other words, fully anonymized CBDC data means no one can identify the exact CBDC user of a given CBDC account. This would dysfunction the whole CBDC project because no one can identify the payer and payee in the transaction to complete the CBDC payment. Therefore, many central banks have expressed the view that CBDC can never be as anonymous as physical cash.[28] Several central banks further cautioned that CBDC could not be completely anonymous or deidentified in light of several public purposes such as AML/CFT as mentioned above.[29] Hence, anonymizing or deidentifying the CBDC data to avoid the application of data protection laws does not appear to be a feasible solution.

Some central banks instead pseudonymize the CBDC data as a protective measure. The two-tier structure adopted by Sweden's e-Krona project is a good example. Riksbank, Sweden's central bank, is conscious of CBDC's privacy concern and thus introduced a special design under which

[25] For studies arguing that issuing central banks would not have much problem complying with their privacy protection obligations, Crowford et al., *supra* note 23, at 164-67.
[26] GDPR, Recital 26.5 and 26.6.
[27] GDPR, Recital 26.3.
[28] Arner et al., *supra* note 2, at 41-42.
[29] *See, e.g.*, BANK OF CANADA ET AL., CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES 6 (2020).

the identity of CBDC users is only known to the authorized operators responsible for KYC and ongoing due diligence. Most importantly, the identity of CBDC users is unknown to Riksbank. Riksbank only receives information on individual account balances and payments but receives no information on the actual account holders.[30] While this design prevents Riksbank from identifying CBDC users directly, it only pseudonymizes, instead of anonymizing, CBDC data. After all, CBDC users can still be identified with the additional information withheld by authorized operators. Therefore, by receiving the information on individual account balances and payments, Riksbank still collects personal data and constitutes a data controller which is subject to data protection laws.[31]

3. A Modified Two-Tier Structure

Another potential method for central banks to avoid the application of data protection laws is a modified two-tier structure. The essence of this structure lies in that central banks delegate the task of ledger administration to partnering institutions.

This structure contains two steps of works. As the first step, a central bank issues the CBDC to its partnering institutions on a wholesale basis. At this stage, the central bank possesses the information related to the CBDC holding of these partnering institutions. This information, however, is merely attributed to these partnering institutions which are legal persons rather than natural persons. Therefore, by far, the central bank has not triggered privacy concerns. As the second step, the partnering institutions transfer the issued CBDC assigned to them to public CBDC users. This move does not subject the central bank to data protection obligations as long as the partnering institutions refrain from passing the data of CBDC users to the central bank.

Under this design, the central bank does not and cannot administer an integrated CBDC ledger because it does not have data attributed to each CBDC user. Instead, it merely possesses the CBDC data attributed to partnering institutions on a wholesale basis. Only the partnering institutions possess the data attributed to public CBDC users and can process it. Data protection laws, if applicable, apply only to partnering institutions and would not extend to the central bank.

The modified two-tier structure replicates the current cash- and deposit-based payment system.[32] 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, incurs data protection obligations. Banks, in turn, possess the deposit information attributed to public depositors and thus undertake related data protection duties. Banks, however, do not pass the information of their depositors to the central bank. Central banks thus avoid being subject to data protection obligations.

---

[30] Raphael Auer et al., *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies*, at 25 (Bank for Int'l Settlements Working Paper, No. 880, 2020).

[31] 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.

[32] For a discussion of the modern payment system, *see* Anton N. Didenko & Ross P. Buckley, *The Evolution of Currency: Cash to Cryptos to Sovereign Digital Currencies*, 42 FORDHAM INT'L L.J. 1041, 1058-61 (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* (BIS Working Papers, No. 698, 2018).

The modified two-tier structure put forward above borrows the logic of the current payment system. The difference is that under the current payment system, banks operate deposit accounts that represent depositors' claims against banks. In contrast, under the modified two-tier structure, banks (or partnering institutions) operate CBDC accounts on behalf of the central bank, which represent direct claims of CBDC users against the central bank. As long as the central bank authorizes the partnering institutions to operate their individual CBDC ledger on its behalf, this arrangement is less of a problem.

The main cost of adopting this structure is that the central bank no longer administers an integrated CBDC ledger. This compromises several functions of CBDC. 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 cannot be as disintermediated because partnering institutions would play a huger 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. In light of these losses, a central bank needs to assess whether this tradeoff is cost-efficient.[33]

C. Designing a Credible Disciplinary Regime

Each of the above three models requires a credible disciplinary regime to ensure that the implementation follows the design. This, in turn, begs the fundamental question of how a domestic regulatory system may effectively supervise and govern central banks to ensure that privacy concerns are being addressed. While achieving that goal would be extremely difficult, it is not entirely impossible. Potential solutions in the domestic context lie in three dimensions: *ex-post congressional oversight*, *special independent supervisory institution*, and *tailor-made data protection regimes*.

Below we present a brief explanation of the 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 to make it possible? Second, who has the power and capability to effectively supervise central banks' compliance with the data protection law and regime? Can a data protection agency undertake that mission? How can the existing data protection laws apply to a central bank? Third, if there is a supervising agency to oversee the central bank, would that contradict the principle of central bank independence? How can we reconcile both objectives?

1. Ex-post Congressional Oversight

The first possible solution is to resort to democratic check-and-balance. This solution builds on the assumption that the issuing central bank will be forced to "line up" with its executive branch of the government. Therefore, only a legislative oversight would have sufficient power to balance that political pressure. In democracies, congress often plays many policy-shaping and agency-

[33] 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 CANADA ET AL., *supra* note 29, at 6.

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 intervention of a central bank's independence. However, this is probably reputable considering the real practice of central bank independence. Central bank independence can mean personnel independence, tenure protection of the governors, and/or freedom in exercising monetary policies, but each of the above requires congressional support in the first place. Therefore, congressional intervention is already inherent in the concept of central bank independence. Admittedly, what we propose in this paper is an *ex-post* and continuous oversight of the central bank by the legislature, which is different from an *ex-ante* appointment or authorization of the central bank leadership and fiscal resources. 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 to have the legislature establish a permanent CBDC privacy safeguard committee that requires the central bank to conduct CBDC-related privacy impact assessment and complaints reporting on a regular basis. This *ex-post* congressional oversight should serve to compel a central bank to obtain the skills to manage the risk accompanied by CBDC circulation. After all, a central bank and other governmental agencies have an incentive to withhold information that may make them culpable for privacy violations. Effective congressional oversight may require a central bank to credibly commit itself to the monitoring of a legislature.

On the other hand, congressional oversight might create room for a political struggle between the ruling party and the opposition, where the incumbents always defend or cover the wrongdoing of a 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. In addition, a central bank should also make regular reports to the multi-partisan committee as proposed above. The committee would then provide an assessment of the data protection performance of the central bank.

Secondly, the legislative committee may be vested with the power to launch investigations. Unlike regular assessments, these investigations shall be targeted at specific events or misconducts. Therefore, this committee may initiate investigations only when there are 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, the legislative committee may 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 institutions.

2. Special Independent Supervisory Institution

The second option is to legislatively establish a special independent institution to oversee the central bank. This institution may consist of consumer representatives, banking associations, experts on IT and cybersecurity, and human rights activists. This option is similar to the previous one to the extent that both options rely on the legislature to take action.

This proposed independent institution, mandated by law and the legislature, may exercise jurisdiction over a central bank's handling of CBDC data or even its data governance regime. In fact, it can be designed as an independent data protector that oversees data governance issues concerning any governmental agencies. In the age of big data and digital transformation, data governance issues have become more pressing and important. Nevertheless, unlike private enterprises, which are generally disciplined by a state's data protection laws and regimes, governmental agencies often fall off the radar. A dedicated independent institution can fill that gap.

Foreseeably, some might respond to this proposed option by arguing that the existing data protection agency may well undertake the task to oversee the central bank. Our counterargument is that, to the extent that these data protection agencies are not independent, it is unrealistic to expect them to adequately supervise other governmental agencies because they may share the same political will with other agencies. To ensure its independence, this independent institution should have a sufficient level of professional staff, particularly the staff's understanding of data security and privacy protection. The staff shall enjoy tenure protection to prevent political interference.

The common problem of an independent supervisory regime is an insufficient authorization. The legislature entrusts the independent institution to supervise, but it might retain the power of making a final assessment, rendering the institution simply an investigatory agency. The legislature may also weaken the institution's independence by blocking the nomination of its executive members. Again, these moves are most likely related to political competition between parties within the legislature. On the other hand, there can be a problem with who watches the watchdog. An overpowered supervisory agency can impede the central bank's governance of CBDC. It can bring stability risk to the financial market if the institution intervenes deeply in the operation of CBDC. Therefore, it would be necessary to design mechanisms that allow the central bank to appeal to a third party. Given the potential bias of the legislative branch, the judicial branch is a better candidate to coordinate and even settle the conflict between a central bank and its supervisory institution.

3. Tailor-Made Data Protection Regime

Last but not least, the data privacy protection regime is always a frontline defense. Most states have their own data privacy laws and regulations. Some are aligned with generally accepted global standards, such as the GDPR in the European Union, whereas some states impose their privacy protection regimes and give certain leeway to governmental agencies.

Although these data protection laws aim at protecting a state's citizens from the misuse of personal data by both the private sector and the government, they generally provide some exceptions or safe harbors for the government due to requirements by laws, purposes of criminal investigations, and/or advancements of public interests. These "public sector waivers" will, to some extent, relieve central banks from the purview of a domestic data privacy law and thus

worsen the privacy concern introduced by CBDCs. Some data protection laws are even inapplicable to governmental agencies.

As a result, this paper argues a need for rethinking the application of privacy law to government agencies and a tailor-made regime for CBDC-issuing central banks. There are a couple of possibilities. First, as elaborated above, a government may consider adopting the modified two-tier structure, which disallows a central bank to access transaction-related information (e.g., payer, payee, the purpose of payments, purchasing items, etc.) and delegate that part to the partnering institutions. Under such a design, the CBDC-issuing central bank will only obtain settlement data as it did under the traditional central bank money and commercial bank money division. The data remains anonymous on the side of the central bank. Such design will cast all privacy law-related compliance burdens on private sector players (i.e., the partnering institutions) and better protect the citizens.

Second, a government may permit the central bank to collect and analyze CBDC data for specific legitimate purposes, such as fostering better, empirically-based decisions about monetary policies. However, it is difficult to draw a fine line between misuse and legitimate use of CBDC data. A tailor-made data protection regime can require the central bank to publish or submit private assessments and board minutes to justify its compliance with related data protection laws, such as the data collection minimization principle and the purpose specification principle. A central bank shall also disclose its cooperation with other governmental agencies, such as law enforcement, to ensure the legitimate use of data. It is also very important that the CBDC-issuing country has in place a comprehensive data governance regime to help itself follow the data protection principles and, most importantly, allow citizens and Parliament to oversee from time to time the central bank's use of personal data.

D. Summary

In this section, we demystify the token-based CBDC and argue that it does not help address the privacy concerns of CBDC. We then analyze three responses potentially adopted by the government, including abiding by the existing privacy laws, anonymizing CBDC data (which is arguably less feasible), and adopting a modified two-tier structure. We finally propose three potential designs to credibly enforce the privacy protection related to CBDCs, including an ex-post congressional oversight, a special independent supervisory institution, and a tailor-made data protection regime. In sum, we argue that there are indeed ways to mitigate CBDC's privacy concerns, but a credible disciplinary mechanism to enforce them is needed.

III. Disciplining CBDC's Privacy Concerns from An International Perspective

All of the preceding analyses focus on the domestic context and attempt to establish a domestic legal framework for addressing CBDC's privacy concerns. These domestic institutions, however, risk failure. After all, building these domestic institutions requires legislative actions, but many countries may lack the political will to prioritize citizens' privacy concerns over other potential utility of CBDC.

In this section, we highlight the possible role of foreign institutions in disciplining CBDCs, particularly the associated privacy concerns. Specifically, as CBDC evolves into an

internationalized payment instrument, it may introduce spillover effects and even infringe the privacy of foreign citizens[34]. This international aspect of CBDC's privacy concerns matters. We will illustrate how the privacy protection regime of a jurisdiction may impose extraterritorial restrictions on another jurisdiction's CBDC and its potential impact on CBDC's ongoing development.

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

Our analyses by far establish that to issue CBDC, a central bank might undertake significant compliance costs to comply with the privacy laws in its jurisdiction. That said, some might argue that these analyses only apply to those jurisdictions that take privacy protection into due account. Admittedly, the intensity of data protection is not the same among all jurisdictions. Therefore, some central banks might be subject to less intensive data protection disciplines and thus undertake little data protection cost in a domestic context. As elaborated in the previous sections, we also admit that establishing a robust domestic mechanism for addressing the privacy concerns caused by CBDC is not an easy task.

That said, modern privacy laws bear the extraterritorial character and thus have the potential to extend to other central banks. GDPR, for instance, represents 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,"[35] it serves as a separate disciplinary mechanism that is highly independent of domestic privacy regulators and thus introduces additional disciplinary effects. Therefore, even if a central bank is subject to minimal data protection disciplines domestically, foreign jurisdictions might impose more intensive 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 his/her 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 B-A-T (i.e., Baidu, Alibaba, and Tencent) in China. To protect the privacy of their citizens or residents, many jurisdictions 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 jurisdictions which witness a significant "export surplus" in data.

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.[36] Based on this mandate, GDPR may apply to data controllers located outside of the European Union.

---

[34] For CBDCs' potential spillover effect, *see* Cheng-Yun Tsang and Ping-Kuei Chen, *Policy Responses to Cross-border Central Bank Digital Currencies – Assessing the Transborder Effects of Digital Yuan*, 17(2) CAP. MKT. L. J. 1-25 (2022).

[35] *See generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020). *See also* Douglas Arner et al., *The Transnational Data Governance Problem*, BERKELEY TECH. L.J. (forthcoming).

[36] GDPR, 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.

In light of this possibility, CBDC issued in a jurisdiction with less rigorous privacy laws is not necessarily immune from the GDPR's disciplines.

Moreover, privacy laws in some jurisdictions apply to public authorities. GDPR, for instance, makes it clear that the data controller subject to its requirements includes the "natural or legal person, *public authority*, *agency or other body* [emphasis added]."[37] Therefore, even if a central bank might claim state immunity to escape the disciplines from domestic privacy laws, it remains subject to privacy disciplines in other jurisdictions.

Admittedly, some existing international institutions might preclude the extraterritorial application of privacy laws of a jurisdiction to foreign central banks. For instance, some data protection agencies might refrain from applying it out of international comity. That said, to the extent that most CBDCs adopt a two-tier structure and thus invite private partnering institutions, these data protection agencies may instead enforce their privacy laws against the partnering institutions. For instance, instead of fining the central bank that issues CBDC, they may suspend the CBDC-related business of the associated partnering institutions in their territories. This indirect disciplinary effect can still have an impact on the issuing central bank.

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

To be sure, there is a precondition for applying the privacy laws of a jurisdiction extraterritorially to the central bank of another jurisdiction. That is, the issuing central bank must collect or process the CBDC data of the citizens of the former jurisdiction. This is a crucial connecting factor. With this connecting factor, a privacy protection agency has a genuine concern that the issuing central bank and its partnering institutions might misuse the CBDC data of its citizens. To ensure the adequate protection of its citizens' CBDC data, it has the motivation and legitimacy to apply its data protection laws to the foreign central bank and/or its partnering institutions.

Accordingly, a central bank may choose to issue CBDC only to its citizens as a response to control the above legal risk. If a central bank only collects and processes the CBDC data of its citizens, it may be less concerned with foreign privacy law and the associated disciplinary effect. Choosing this way, however, necessarily discourages the issued CBDC from serving a cross-border payment instrument. Moreover, the central bank cannot reap the currency internationalization function of CBDC as well. If these international aspects of functions remain on the agenda of the issuing central bank, it has to more or less address the privacy concerns of its CBDC even if domestic laws do not require so.

Based on this observation, we wish to raise an international gaming perspective. The preceding analyses have established the case that privacy laws, especially the Brussels Effect of privacy laws, may serve as a practicable tool to inhibit the CBDCs of other jurisdictions. In this global CBDC competition, some jurisdictions apparently have taken the lead while others remain lagging behind. The follower jurisdictions, however, may use their privacy laws as a weapon to preclude other developed CBDCs from evolving into cross-border payment instruments. At the

[37] GDPR, art. 4(7).

minimum, they may prevent other developed CBDCs from entering into their domestic markets and thus preserve the space for developing their native CBDCs.

Then what would the world be if most major jurisdictions exerted this Brussels Effect and extended their privacy laws to CBDCs of other jurisdictions? If this move becomes common practice among world privacy protection agencies and thus ousts foreign CBDCs from their domestic markets, each CBDC system would become isolated islets that only serve their domestic markets and payment needs. It would be costly to exchange one CBDC with another. In the end, no CBDC can evolve into a globally-accepted cross-border payment instrument.[38]

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. Other potential beneficiaries would be the emerging cross-border payment instruments. Global stablecoins, for instance, might have some edge, particularly if the issuer volunteers to undertake the compliance costs, including those arising from financial supervision and privacy protection requirements.

Is this a happy ending? We are doubtful. Nevertheless, if major sovereigns do not wish to simply position their CBDCs as a local payment instrument, they will have to figure out ways to mitigate the Brussels Effect of the existing privacy protection laws. Considering that the said Brussels Effect results from the unilateral yet extraterritorial application of laws, major sovereigns may start by exploring bilateral, plurilateral, or even multilateral dialogues to harmonize the impact of domestic privacy laws.[39] The evolving cross-border privacy initiatives or forums, digital trade chapters in free trade agreements, digital economy agreements, etc., might have the potential to provide the platform for these mutual dialogues.[40]

IV. Concluding Remarks

In the coming years, CBDCs might innovate payment systems, reduce frictions of cross-border money transferring, enhance social welfare and empower central banks. Nevertheless, these aspirations do not come without costs or problems. Many regulatory ones need to be addressed, particularly on privacy protection. As any person would readily appreciate, unlike cash, digital cash, like a CBDC, can track trails of citizens' transactions and, therefore, may well infringe on citizens' privacies. The issuing central bank might sometimes be required by its government or other governmental agencies to share CBDC data it enjoys or has access to. Such a scenario will subject citizens' privacy to significant risks. Some disciplinary safeguards must be in place to prevent that from happening, but the unsettled problem is how we can design these safeguards without jeopardizing central banks' 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. That said, we also

[38] 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 35, at 47-53.
[39] For a discussion of these different approaches to establish cross-border privacy cooperation, *see id.* at 57-65.
[40] For a discussion of the potential driving force and resistance of these cross-border privacy arrangements, *see, e.g.*, Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 165-78 (2017).

recognize the fact that building these domestic regimes requires legislative actions. Still, many countries 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 foreign institutions in disciplining CBDC-issuing central banks and their governments under modern privacy protection laws. This paper notes some modern privacy laws that impose the so-called Brussels Effect, resulting in the unilateral and extraterritorial application of laws onto foreign CBDC-issuing governments. We anticipate major sovereigns may start by exploring bilateral, plurilateral, or even multilateral dialogues to harmonize the impact. Thus, if properly designed, applying modern privacy laws and proper supporting mechanisms may serve as effective disciplines on CBDCs and their issuing central banks.