Michigan Journal of International Law

Volume 42 | Issue 2

2021

The Privacy Cost of Currency

Karin Thrasher
University of Michigan Law School

https://doi.org/10.36642/mjil.42.2.privacy

THE PRIVACY COST OF CURRENCY

*Karin Thrasher**

I. INTRODUCTION

Most central banks issue two types of money: banknotes and reserve deposits.[1] Banknotes, or cash, can be used continuously by any person for nearly every transaction, and provide anonymity for the parties. Meanwhile, reserve deposits are largely restricted to a limited number of entities and banks. These reserve deposits are used for large-value-settlement.[2] However, as digitization increases, the role and form of money is changing.[3] In response to pressure produced by the increase in new forms of money and the potential for a cashless society, states are exploring potential substitutes to cash. Governments have begun to investigate the intersection of digitization and fiat currency: Central Bank Digital Currencies ("CBDC").[4]

Before discussing CBDCs, it is vital to recognize the role cash plays in the modern financial system. The greatest attribute of cash is that it carries only the information of value, protecting purchaser privacy.[5] Cash is the only established payment system that scored "full anonymity" in the International Monetary Fund's ("IMF") survey on CBDC; cash protects privacy because no account is required, and there is no record of transactions.[6] Even central banks, the issuer of legal tender fiat currency, cannot know who pos-

---

* J.D. Candidate, University of Michigan Law School (2021); B.A., University of California, Los Angeles (2018). My sincere thanks to Professor Veronica Santarosa for helping me conceptualize this paper in 2019. I also thank Professor Adrienne Harris, Christie Baer, and Emma Macfarlane at the Center on Finance, Law, and Policy, for the introduction to, and insights on, this topic. Finally, I am grateful for the stellar editing and support of the editorial staff at *MJIL*—of whom I would especially like to thank Alessandro Storchi for his invaluable edits.

1. Noriyuki Yanagawa & Hiromi Yamaoka, *Digital Innovation, Data Revolution, and Central Bank Digital Currency* 2 (Bank of Japan Working Paper Series No. 19-E-2, 2019).

2. *See id.*

3. Christine Lagarde, IMF Managing Dir., Address at the Singapore Fintech Festival: Winds of Change: The Case for a New Digital Currency 2 (Nov. 14, 2018), https://www.imf.org/~/media/Files/News/Speech/111418-md-sg-fintech-speech.ashx?la=en.

4. *See id.* at 3 (explaining that "Various central banks around the world are seriously considering these ideas, including Canada, China, Sweden, and Uruguay. They are embracing change and new thinking—as indeed is the IMF.").

5. *See* G45, WORLD CASH REPORT 4 (2018).

6. *See* TOMMASO MANCINI-GRIFFOLI, MARIA SOLEDAD MARTINEZ PERIA, ITAI AGUR, ANIL ARI, JOHN KIFF, ADINA POPESCU, & CELINE ROCHON, IMF STAFF DISCUSSION NOTE: CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY 39 (Nov. 2018).

sesses cash.[7] Cash continues to be the favored payment instrument for individuals who seek anonymity in their transactions,[8] and remains the most widely used payment instrument.[9] However, the availability of alternate payment structures is growing; in particular, the rate at which electronic payment transactions volumes are increasing is outpacing the rate at which cash is used.[10] In sum, this results in cash holding a progressively smaller share of the payments market.[11]

Cash, while praised for its clear compliance with international privacy standards, is not without pitfalls. In the financial system, cash is scrutinized for its role in money laundering and terrorist financing; the international requirements for compliance in these areas are continuously evolving.[12] Cash allows for transactions with complete anonymity.[13] Complete anonymity, however, comes with trade-offs.[14] Cash is a successful medium for illegal activity, such as money laundering, terrorist financing, and tax evasion.[15] Importantly, the elimination of cash would increase the cost of these illicit activities.[16]

While the desire to limit money laundering and terrorist financing through reducing the availability of cash is widely recognized as valid, states "do not owe any customary international law obligations with respect

---

7. *See* David Winning & James Glynn, *The World's Cash is Disappearing. Bankers Aren't Sure Where It Went*, WALL ST. J. (Dec. 12, 2019, 4:01 PM) https://www.wsj.com/articles/the-worlds-cash-is-disappearing-bankers-arent-sure-where-it-went-11576184491.

8. *See* ECB Crypto-Assets Task Force, *Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures* (Occasional Paper Series, No. 223/ May 2019).

9. *See* G45, *supra* note 5, at 4.

10. *See id.* at 15.

11. *See generally id.* at 15.

12. Mercy W. Buku & Michael W. Meredith, *Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity*, 8 WASH. J. L. TECH. & ARTS 375, 394 (2013).

13. Société Universitaire Européenne de Recherches Financières ["SUREF"], *Do We Need Central Bank Digital Currency? Economics, Technology, and Institutions*, 2018/2 SUERF Conf. Proceedings 28 (2018).

14. Some authors have suggested that a coordinated international regulation of money forms that provide anonymity, such as cryptocurrencies, could assist in reducing the evasion of sanctions, terrorist financing, and tax evasion. These proposals, however, sacrifice the international right to privacy in the process, showcasing the inherent tension between privacy and illegal activity. *See, e.g.*, Emma Macfarlane, Note, *Strengthening Sanctions: Solutions to Curtail the Evasion of International Economic Sanctions Through the Use of Cryptocurrency,* 42 MICH. J. INT'L L. 199 (2020).

15. *See* SUREF, *supra* note 13, at 28.

16. *See generally* Emanuele Borgonovo, Stefano Caselli, Alessandra Cillo, Donato Masciandaro & Giovanni Rabitti, *Cryptocurrencies, Central Bank Digital Cash, Traditional Money: Does Privacy Matter?* 7 (Ctr. for Applied Rsc.h on Int'l Markets, Banking, Fin., and Regul. Working Paper No. 95, 2018) (noting that "[a]mong the individuals that like the anonymity property are people who appreciate this property for illegal reasons, as an anonymous currency can be an effective device for money laundering.").

to the protection of other countries' monetary systems" aside from the duty to prevent counterfeiting.[17] This balancing between domestic legislation to limit the channels available for illicit activities and the international requirement to protect the fundamental right to privacy creates a fundamental tension.

Jurisdictions have begun researching and developing CBDCs to serve in lieu of cash.[18] Some central banks are analyzing the potential for a CBDC that could be made available to the public and serve as a substitute for cash by providing an alternate, safe, and robust payment instrument.[19] The acknowledgement by international bodies that a world without cash is imaginable has encouraged the development of CBDCs.[20] However, eliminating cash would undermine privacy of individuals.[21] The creation of a CBDC in response to the potential cashless society raises the question whether the anonymity previously provided by cash must be safeguarded by the state.

This note will conclude that a central bank in a cashless society must opt for the token-based form of CBDC, which provides the most privacy to individuals. States that choose an account-based CBDC will be in violation of fundamental international privacy principles. Part I of the note will provide an overview of Central Bank Digital Currencies, drawing the crucial distinction between account-based and token-based currencies. Part II will establish that the broad right to privacy in the digital age is inclusive of personal financial data and elaborate on the right to privacy specifically involved by financial transactions, describing the derivation of the lawful and arbitrary standards from article 17 of the International Covenant on Civil and Political Rights ("ICCPR"). Part III will conclude that while the lawful standard of article 17 is not dispositive of account-based CBDCs, the relevant factors lean in favor of token-based CBDCs. The favor of token-based CBDCs will be solidified in Part IV, where account-based CBDCs will be shown to be arbitrary, in violation of article 17. Finally, Parts V and VI will provide policy implications and concluding thoughts.

---

17. Charles Proctor, *Cryptocurrencies in International and Public Law Conceptions of Money*, *in* CRYPTOCURRENCIES IN PUBLIC AND PRIVATE LAW 33, 40 (David Fox & Sarah Green eds., 2019).

18. *See* SVERIGES RIKSBANK, THE RIKSBANK'S E-KRONA PROJECT REP. 1 at 4 (2017) (explaining that Sweden has begun to see a decline in the use of cash, but that those developments are unique from an international perspective).

19. *See* BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENTS & MKT. INFRASTRUCTURES ["CMPI"], CENTRAL BANK DIGITAL CURRENCIES 7 (2018) https://www.bis.org/cpmi/publ/d174.pdf.

20. *See* Yanagawa & Yamaoka, *supra* note 1 at 5; *see also* Raphael Auer & Rainer Böehme, *The Technology of Retail Central Bank Currency*, BIS Q. REV., Mar. 2020, at 85, 86–87.

21. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 20.

II. THE STRUCTURE OF CENTRAL BANK DIGITAL CURRENCIES

A CBDC does not yet have a precise definition because of the wide variation in form that the instrument can take. Despite the lack of a specific definition, a CBDC has been proposed by several sources as a "widely accessible digital form of fiat money that could be legal tender."[22] There are four key factors in distinguishing a CBDC: issuer, accessibility, form, and technology used.[23]

First, as the name suggests, a CBDC is issued by the central bank.[24] Second, CBDCs can be either widely accessible to individuals similar to cash or bank deposits, and thus meant for general purpose, or can be restricted to a limited number of financial institutions and banks, and thus meant for wholesale purposes only.[25] A general purpose CBDC is designed to be widely accessible to households and businesses without the involvement of a bank intermediary.[26] This note will focus only on general-purpose forms of CBDCs. The wholesale form of a CBDC is more akin in function to central bank reserves and is outside the scope of this note. Third, the currency takes a digital form, as opposed to a physical currency such as cash.[27] The fourth factor, the technology employed, is the main point of divergence between the different types of CBDC.[28] There are two basic potential systems: a token-based currency, or an account-based currency.

A token-based currency is characterized by a few key distinctions that allow for the provision of anonymity.[29] First, a token-based currency would likely utilize a cryptographic scheme that does not require user identification.[30] Second, the token-based currency would likely use some form of dis-

---

22. *See id.* at 4.

23. *See* Christian Barontini & Henry Holden, *Proceeding with Caution—A Survey on Central Bank Digital Currency* 1 (Bank for Int'l Settlements, BIS Papers No. 101, 2019).

24. *See* WORLD BANK, DISTRIBUTED LEDGER TECHNOLOGY (DLT) AND BLOCKCHAIN FINTECH NOTE NO. 1 4 (2017).

25. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 7.

26. *See* Lael Brainard, Bd. of Governors of the Fed. Rsrv. Sys., Remarks on the Monetary Policy, Technology, and Globalization Panel at Monetary Policy: The Challenges Ahead, an ECB Colloquium (Dec. 18, 2019).

27. *See* Hossein Nabilou, *Central Bank Digital Currencies: Preliminary Legal Observations*, J. BANKING REGUL. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329993.

28. *See* Tammaro Terracciano & Luciano Somoza, *Central Bank Digital Currency: The Devil is in the Details,* LSE BUS. REV. (May 26, 2020), https://blogs.lse.ac.uk/businessreview/2020/05/26/central-bank-digital-currency-the-devil-is-in-the-details/ (arguing the two key distinctions in types of Central Bank Digital Currencies ("CBDC") are token-based and account-based technologies, and single-tier and two-tier distribution systems).

29. *See id.* (noting that in a token-based CBDC, it is technologically possible to implement a system of anonymous offline transactions).

30. *See* Nabilou, *supra* note 27, at 17 (citing Yves Mersch, Member Executive Board of the ECB, Digital Base Money: An Assessment from the ECB's Perspective*,* Speech at the

tributed ledger technology ("DLT").[31] DLT's important contribution in the formation of currency is the provision of a system that allows for trust among anonymous participants without any need for trust across institutions.[32]

An account-based CBDC requires a central party—the central bank.[33] The account-based system involves a transfer of a claim on an account.[34] In this system, the user would request a transfer of funds between accounts held at the central bank. The central bank would then ensure settlement, but only after verification of authority to use the account, and authenticity of the recipient's account.[35] Thus, the account-based system requires a much larger exchange of information than a token-based system.

The level of anonymity associated with each of these technologies is a key concern for designers of CBDC.[36] Further, the appropriate degree of privacy is a challenge in a digital environment and demands careful consideration of public policy design choices.[37]

Throughout the discussion of applicability of international privacy law, it is precarious to equate CBDCs to other forms of virtual currencies because CBDCs face the unique threat of mass centralization and data collection.[38] The CBDC's issuer is the most impactful factor on privacy implications when compared to other virtual currencies. While CBDCs are issued and governed by the country's central bank, other virtual currencies are governed by disparate online communities.[39] Because CBDCs are issued by central banks and require reliance on the central bank for full functionality, large amounts of sensitive information will accumulate.[40] In particular, in an account-based CBDC system, all transactions of citizens will be visible to

---

Farewell Ceremony for Pentti Hakkarainen (Jan. 16, 2017)); Auer & Böehme, *supra* note 20 at 86–87.

31. SANTIAGO FERNÁNDEZ DE LIS & JAVIER SEBASTIÁN, CENTRAL BANK DIGITAL CURRENCIES AND DISTRIBUTED LEDGER TECHNOLOGIES 1 (2019).

32. *See* WORLD BANK, *supra* note 24, at 2.

33. CPMI, *supra* note 19, at 4

34. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 8.

35. *See* WORLD BANK, *supra* note 24, at 7.

36. *See* Chen Ye & Kevin C. Desouza, *The Current Landscape of Central Bank Digital Currencies*, BROOKINGS (Dec. 13, 2019), https://www.brookings.edu/blog/techtank/2019/12/13/the-current-landscape-of-central-bank-digital-currencies/.

37. CPMI, *supra* note 19, at 10.

38. *See* Tom Wilson, *Explainer: Central Bank Digital Currencies—Moving Towards Reality?*, REUTERS (Jan. 23, 2020), https://www.reuters.com/article/us-cenbank-digital-currencies-explainer/explainer-central-bank-digital-currencies-moving-towards-reality-idUSKBN1ZM2JH (explaining that CBDCs are fundamentally different than cryptocurrencies because of their status as legal tender); *see also* Linda M. Schilling, École Polytechnique CREST, Speech prepared for Reinventing Bretton Woods Committee: Risks Involved with CBDCs: On Cash, Privacy, and Information Centralization, (Oct. 29–30, 2019).

39. *See* Wilson, *supra* note 38.

40. *See* Schilling, *supra* note 38, at 3.

the central bank. This system creates a greater central accumulation of sensitive information than in the current system of segmented multiple private banks collecting information on customers.[41]

While no state is yet to proffer a permanent CBDC, the idea is at the forefront of state-based innovation across jurisdictions and multilateral institutions. A majority of central banks have begun researching CBDCs.[42] Several central banks have begun studying the concept, and a few states have undertaken pilot programs to more fully explore the idea.[43] Overall, roughly seventy percent of respondents to the 2018 Bank for International Settlements survey reported that they were engaged in CBDC work.[44]

The reasons driving the development and research of CBDCs vary based on the status of the state. Developed states are investigating CBDCs to increase payment safety and efficiency, whereas emerging market economies are creating CBDCs to facilitate financial inclusion.[45] Crucially for the analysis of a CBDC under the international privacy framework, some advanced economies are motivated by the prospect of a cashless state which may allow for increased public utility.[46] Further, central banks are anticipated to be encouraged by currency forms that support "monetary policy, financial stability, and integrity."[47]

III. THE BROAD RIGHT TO PRIVACY IN THE DIGITAL AGE

A. *International Privacy Framework*

The rise of CBDCs, and variance in technology used to create the currency, raises the question of which form, if any, may best comply with International Privacy Law standards. For example, Sweden has researched both an account-based and a token-based e-krona and is proceeding in contracting a consulting company, Accenture, to develop the currency plan further.[48] The Tunisia initiative, promoted directly by the government, issued

---

41. *Id.* at 4.

42. *See* Barontini & Holden, *supra* note 23, at 11.

43. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 27; *see also* Yanagawa & Yamaoka, *supra* note 1, at 9.

44. *See* Barontini & Holden, *supra* note 23, at 7.

45. *See id.* at 9.

46. *See* Emanuele Borgonovo, Stefano Caselli, Alessandra Cillo, & Donato Masciandaro, *Beyond Bitcoin and Cash: Do We Like a Central Bank Digital Currency? A Financial and Political Economics Approach* 2 (Ctr. for Applied Rsch. on Int'l Markets, Banking, Fin., & Regul., Working Paper No. 65, 2017) (explaining that public utility of cash is disputed, as cash has two important drawbacks: contribution to the illegal economy, and hampering monetary policy).

47. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 4.

48. *See generally* Sayuri Shirai, *Central Bank Digital Currency: Concepts and Trends*, VOX CEPR POL'Y PORTAL (Mar. 6, 2019), https://voxeu.org/article/central-bank-digital-

retail tokens based on a distributed ledger.[49] These examples are not exhaustive: Uruguay and the People's Republic of China have also piloted their own unique forms of CBDCs.[50]

The global development of CBDCs raises many legal concerns; one of the most predominant questions is the appropriate degree of privacy that should be afforded to users of the currency.[51] International privacy law presents a set of concise, binding standards that states must take into consideration when determining what framework should regulate the issuance of a CBDC. Privacy is a fundamental human right recognized throughout international bodies and treaties.[52] The first modern recognition of the importance of privacy at the international level came with the 1948 Universal Declaration of Human Rights ("UDHR"). Article 12 of the UDHR states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[53] This first pronouncement on the right to privacy showcases that the existence of the right to privacy has been considered necesnecessary and uncontested from the drafting of the UDHR.[54]

The right to privacy became legally binding on states that ratified the International Covenant on Civil and Political Rights ("ICCPR"). Article 17

---

currency-concepts-and-trends (explaining that "The Riksbank has been actively considering the first two proposals under the 'e-krona' project. The first, 'account-based retail CBDC' proposal is the issuance of a digital currency to the general public in the form of directly providing an account at Riksbank. The second, [is the] 'value-based retail CBDC.'").

49. *See* Sayuri Shirai, *Money and Central Bank Digital Currency* (Asian Dev. Bank Inst. Working Paper No. 922, 2019), https://www.adb.org/sites/default/files/publication/485856/adbi-wp922.pdf.

50. *See* Alun John, *Explainer: How Does China's Digital Yuan Work?,* REUTERS (Oct. 19, 2020), https://www.reuters.com/article/us-china-currency-digital-explainer/explainer-how-does-chinas-digital-yuan-work-idUSKBN27411T; *see also* Marie Huillet, *People's Bank of China Progressing Smoothly with Digital Yuan,* COINTELEGRAPH (Jan. 6, 2020), https://cointelegraph.com/news/peoples-bank-of-china-progressing-smoothly-with-digital-yuan. *See generally* Gerardo Licandro, Uruguayan e-Peso on the Context of Financial Inclusion (Nov. 16, 2018), https://www.bis.org/events/eopix_1810/licandro_pres.pdf.

51. *See* CPMI, *supra* note 19, at 9–10.

52. *Compare* International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter "ICCPR"], *with* G.A. Res. 217(III)A, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter "UDHR"]. *See generally* PROMOTIONAL PRODUCTS ASS'N INT'L, THE GENERAL DATA PROTECTION REGULATION (2018), https://www.ppai.org/media/2941/gdpr.pdf.

53. *See* UDHR, *supra* note 52, art. 12.

54. *The Right to Privacy and Family Life*, ICE. HUM. RTS. CTR., http://www.humanrights.is/en/human-rights-education-project/human-rights-concepts-ideas-and-fora/substantive-human-rights/the-right-to-privacy-and-family-life (last visited Apr. 5, 2020). There was no discussion debating whether or not to include the right to privacy. This indicates a guarantee that privacy would be included in some form. *See* U.N. Secretary-General, *Annotations on the Text of the Draft International Covenant on Human Rights*, ¶ 99, U.N. Doc. A/2929 (July 1, 1955).

of the ICCPR states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[55] This binding provision is worded almost identically to the UDHR, with the sole difference between the two being that ICCPR article 17 prohibits not only "arbitrary" interferences with one's privacy, but also "unlawful" ones.[56]

B. *The Right to Privacy in the Digital Age*

The existence of an internationally recognized right to privacy, coupled with the broad interpretations promulgated in international courts, inherently acknowledges the existence of certain areas of an individual's life that should be outside the scope of the state. The Human Rights Committee and regional human rights bodies interpret the right to privacy broadly through jurisprudence, commentary, and emerging state practices. The Inter-American Court of Human Rights has held that the private sphere is "exempt from and immune to abusive or arbitrary interference or attacks" by both public and private actors.[57] Further, in *Murillo v. Costa Rica*, the court noted that the scope of protection of the right to privacy has been and should be interpreted in broad terms by the international human rights courts.[58] In *Rosendo Cantu v. Mexico*, the court has affirmatively described the right to privacy as a "wide-ranging term, which cannot be exhaustively defined."[59] The broad adaptions of the right to privacy, stemming from article 17 of the ICCPR, suggest that the right is framed to protect a range of actions that fall within the private sphere of an individual's life.

The right to privacy includes the right to one's person and identity.[60] The modern interpretation of identity includes the consideration of a person's digital identity.[61] International organizations have warned about the impact of experimental technology on the right to privacy. The Committee of Ministers of the Council of Europe holds that the privacy of individuals

---

55. ICCPR, *supra* note 52, art. 17.

56. *See generally* Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441, 449 (July 7, 2014).

57. Murillo v. Costa Rica, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 257, ¶ 142 (Nov. 28, 2012) (explaining that the private sphere encompasses a wide range of factors associated with individual dignity, including but not limited to the right to autonomy, development and the right to establish and develop relationships with others, and the way the individual views themselves).

58. *See id.* ¶ 142.

59. Rosendo Cantu v. Mexico, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 216, ¶ 119 (Aug. 31, 2010).

60. *See The Right to Privacy and Family Life*, *supra* note 54.

61. *See* Org. Econ. Cooperation & Dev. ["OECD"], *At a Crossroads: "Personhood" and Digital Identity in the Information Society* 7 (OECD Directorate for Science, Technology and Industry STI Working Paper 2007/7, 2008).

should be guaranteed "in any research project requiring the use of personal data."[62] Our online interactions challenge the traditional notions of privacy; as interactions using technology increase, individuals are more vulnerable to breaches of privacy.[63] These considerations of personal digital identities and online data must be considered when determining whether an action infringes on the right to privacy.

The United Nations anticipated the inherent tension that could arise between the right to privacy and technological developments.[64] Even in 1976, the Human Rights Commission suggested that developing international standards to protect the right to privacy was well within their competence, especially considering the impact of technological developments, such as recording.[65] This discussion highlights a consensus that technology should not be permitted to infringe on the areas of the private sphere that are exempt from interference by public and private actors.

Since the adoption of article 17 of the International Covenant on Civil and Political Rights, the United Nations has undertaken resolutions to further explain the right to privacy. In January 2014, the United Nations General Assembly adopted resolution 68/167.[66] This resolution both called on states to protect the right to privacy in the digital age and noted that international human rights law provides the structure to examine instruments' and actions' compliance with the right to privacy.[67] The Special Rapporteur on the right to privacy found that while many jurisdictions committed themselves to protecting the right to privacy through the ICCPR, many of them simultaneously put the right at risk by employing new, but incompatible, technologies.[68] This acknowledgement of the riskiness of new technologies suggests that adoption of a CBDC could be considered an infringement if it sufficiently interferes with the right to privacy.

Instead of putting the right to privacy at risk, the OHCHR instructs that "privacy by design and default should be a central element for developing

---

62. Council of Eur., Comm. of Ministers, *On the Protection of Personal Data Used for Scientific Research and Statistics*, ¶ 2.1, App. to Recommendation R(83)10, (Sept. 25, 1983).

63. *See generally* DEP'T PRIME MINISTER & CABINET, AUSTL., CONNECTING WITH CONFIDENCE: OPTIMISING AUSTRALIA'S DIGITAL FUTURE 11 (2011), http://indianstrategicknowledgeonline.com/web/connecting_with_confidence_public_discussion_paper.pdf.

64. *See* Comm'n Human Rights, Rep. on the Thirtieth Session, U.N. Doc. E/CN.4 /1116, at 10 (1976).

65. *See id.*

66. *See generally* G.A. Res. 68/167, The Right to Privacy in the Digital Age (Jan. 21, 2014).

67. *See* U.N. CONF. ON TRADE & DEV. ["UNCTAD"], DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT 24 (2016).

68. *See* Rep. of the Special Rapporteur on the Right to Privacy, *Right to Privacy,* ¶ 8, U.N. Doc. A/HRC/40/63 (2019).

new technologies."[69] Developers are instructed to identify privacy implications before and during the development process.[70] This instruction extends to the creators of CBDC, and charges them with the responsibility of considering the varying privacy risks between types. While the right to privacy is not absolute, any instance of infringement must be critically examined to determine the infringement's compliance with minimum impairment, legitimacy, and proportionality.[71]

Considering the guidance protecting the right to privacy in a digital age, the security and privacy of an individual's financial data should be heavily scrutinized due its sensitive, and potentially valuable, nature.[72] In analyzing the retention of personal data, the Court of Justice of the European Union in *Digital Rights Ireland Ltd. v. Minister of Communications* noted that the "protection of personal data [. . .] is especially important for the right to respect for private life."[73] The development of a CBDC would create an unprecedented aggregate of personal financial data, leading to increased vulnerability to cyber-attacks.[74] The aggregation and centralization of sensitive personal data should be monitored by the international privacy frameworks. Currently, privacy considerations such as the restrictions on the usage of personal financial data by third parties are applied to digital money accounts.[75] The introduction of CBDCs and supporting technology requires an analysis of the new technical architecture to ensure privacy of financial data.[76]

C. *Testing Whether an Action Infringes on the Right to Privacy*

Only a few decades ago, treaties promulgating fundamental human rights, including the right to privacy, were not seen as an instrument in resolving data privacy issues.[77] This trend has shifted: The right to privacy is now the center of discussions surrounding data privacy. Today, article 17 of the ICCPR is commonly viewed as providing the basis for modern data pri-

---

69. *See* INT'L NETWORK C.L. ORG., THE RIGHT TO PRIVACY IN THE DIGITAL AGE, HUMAN RIGHTS COUNCIL ADOPTED RESOLUTION 34/7 4 (2018).

70. *See id.*

71. *See* UNCTAD, *supra* note 67, at 24.

72. *See* INT'L TELECOMM. UNION ["ITU"], REGULATORY CHALLENGES AND RISKS FOR CENTRAL BANK DIGITAL CURRENCY 13 (June 2019).

73. *See* Joined Cases C-293/12, C-594/12, Digit. Rts. Ir. Ltd. v. Minister of Commc'ns, Marine, & Nat. Res. et al., ECLI:EU:C:2014:238, ¶ 53 (Apr. 8, 2014).

74. *See* Schilling, *supra* note 38, at 4.

75. *See* ITU, *supra* note 72, at 14.

76. *See id.* (explaining the "broad social implications of digital technology necessitate that privacy issues, including the appropriate balance between anonymity and law enforcement, should be deliberated").

77. *See* LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 82 (2014).

vacy law, together with the resulting jurisprudence.[78] As such, article 17 and its interpretation will serve as the basis for analyzing international privacy standards for CBDCs in this note. The framework developed in article 17 of the ICCPR determines whether there has been an infringement on the right to privacy. Article 17 states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation."[79] The analysis of privacy law is conducted under the ICCPR because, as a convention, it is legally binding for signatories.[80] Further, the ICCPR has had the strongest impact on the national level, exerting legal order on the same governments that are exploring and piloting CBDCs.[81] The states bound by the ICCPR are bound primarily by negative obligations, and must refrain from interfering with an array of protected rights.[82]

The language of article 17 draws a distinction between fundamental rights that are protected only from unlawful interference, such as honor, and rights that are protected from unlawful *and* arbitrary interference, such as privacy.[83] This language differs from the UDHR article 12 language, in which the term unlawful is not present. The two key terms that qualify the prohibited interference are then "arbitrary" and "unlawful." When adopting language from article 12, the ICCPR drafters chose to prohibit arbitrary interference with privacy, home, and correspondence, but eliminated the prohibition on arbitrary interference on honor, which was present in article 12.[84] The language of article 17 shows that the drafters consciously maintained the protection on arbitrary interference on the right to privacy, while eliminating the protection from other rights. Fundamentally, the addition of "unlawful" and maintenance on "arbitrary" suggests both terms should be given equal weight when determining whether an instrument or act is in violation of international privacy law.

As initially explored in *Van Hulst v. Netherlands,* for an interference with the right to privacy to be "non-arbitrary," it must satisfy a four-part test: (1) pursuance of a legitimate aim, (2) rational connection to the legitimate aim, (3) minimal impairment to the right of privacy, and (4) proportionality between the pursuit of the legitimate aim and the limitation of the

---

78. *See id.* at 82–84.

79. *See* ICCPR, *supra* note 52, art. 17.

80. *See id.*

81. Christion Tomuschat, *Introductory Note: International Covenant on Civil and Political Rights,* AUDIOVISUAL LIBR. INT'L L. (2008), https://legal.un.org/avl/ha/iccpr/iccpr.html.

82. David Sloss, *The Domestication of International Human Rights: Non-Self-Executing Declarations and Human Rights Treaties*, 24 YALE J. INT'L L. 129, 138 (1999), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1099&context=yjil.

83. *See* ICCPR, *supra* note 52, art. 17.

84. *See* UDHR, *supra* note 52, art. 12.

right to privacy.[85] The UN Human Rights Committee ("HRC") released further guidance on the interpretation of article 17 through General Comment 16.[86] General Comment 16 states that "[t]he introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the covenant and should be, in any event, reasonable in the particular circumstances."[87]

Any suspected interference is subject to the arbitrary analysis, in effect requiring the interference to pass both the four-part proportionality assessment as well as the reasonable circumstances assessment.

General Comment 16 also elaborates on the lawful requirement, clarifying that an interference on the right to privacy can only occur "on the basis of law" that is consistent with "the provisions, aims, and objectives of the covenant."[88] This analysis applies to both international law and domestic law.[89] The domestic law must be accessible and foreseeable.[90] Further, the domestic law must be precise and clearly defined.[91] Thus, the lawfulness standard also has, in effect, a four-part test: (1) consistency with the covenant, (2) pursuance to domestic and international law, (3) accessibility, and (4) clear definition. All of these standards, coupled with the four-part arbitrary test, explained above, must be met in order for an infringement on the right to privacy to be acceptable under article 17's text.

---

85. *See* Van Hulst v. Netherlands, U.N. Hum. Rts. Comm. 82d Sess., Commc'n No. 903/1999, ¶¶ 7.3, 7.6, 7.10, U.N. Doc. CCPR/C/82/D/903/1999 (HRC 2004); *see also* AM. C. L. UNION ["ACLU"], PRIVACY RIGHTS IN THE DIGITAL AGE: A PROPOSAL FOR A NEW GENERAL COMMENT ON THE RIGHT TO PRIVACY UNDER ARTICLE 17 OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 25 (2014), https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf.

86. *See generally* Off. High Comm'r for Hum. Rts., General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, HRI/GEN/1/Rev.9 (Vol. 1) (Apr. 8, 1988) [hereinafter General Comment 16].

87. *See id.* ¶ 4.

88. *See id.* ¶ 3.

89. *See* ACLU, *supra* note 85, at 21, citing Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 56 (2009); *see also* Kennedy v. United Kingdom, App. No. 26839/05, Judgment, Eur. Ct. H.R., 207, 253 (2010).

90. *Kennedy,* 52 Eur. Ct. H.R. at 253.

91. *Compare* Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Comments, Russian Federation, ¶ 19 U.N. Doc. CCPR/C/79/Add.54 (July 26, 1995) (explaining that mechanisms to intrude into a private communication still exist without clear legislation), *with id.* ¶ 31 (recommending that the relationship between bodies charged with protection of human rights be clearly defined, and that a mechanism to ensure conformity with the convention is established).

V. THE APPLICATION OF THE LAWFUL STANDARD TO ACCOUNT-BASED AND TOKEN-BASED CBDCS

While both token-based and account-based CBDCs should be analyzed under article 17, it is important to recognize that the forms present inherently different privacy risks due to the structure of the technology. The predominant distinction between account-based and token-based general purpose CBDCs is that account-based CBDCs employ intermediates to verify the identity of the purchaser, while token-based CBDCs use tokens that are verified by the receiver.[92] Any CBDC would likely look different than a permissionless, peer-to-peer model seen in currencies like Bitcoin.[93] However, even the United States' Federal Reserve Board recognizes that an account-based model where the central bank issues a CBDC directly to consumer accounts would raise huge legal questions, presumably concentrated within the privacy framework.[94] The central bank in an account-based system would be privy to all citizens' financial data, allowing the central bank to view sensitive transactions.[95] While the token-based model of CBDCs would raise considerable regulatory and policy questions, it is possible that the issuing central bank, through applying DLT and encryption technologies, could realize anonymity in order to protect the privacy of the individual consumers.[96] The account-based CBDC presents a higher level of government interference with personal financial data, and provides the individual with less privacy.

To test whether a general-purpose CBDC is lawful under article 17, the currency should be evaluated on four requirements: (1) consistency with the covenant, (2) pursuance to domestic and international law, (3) accessibility, and (4) clear definition. The first prong holds that in whatever form it takes, the CBDC must be consistent with the aims and goals of the ICCPR. article 17 should be read in light of General Comment 16, which provides that laws that permit interference should be "in accordance with the provisions, aims and objectives of the covenant."[97] When article 17 was being considered, there was no dispute as to the principle involved because "privacy, the sanctity of the home, the secrecy of correspondence and the honour and reputation of persons were protected under the constitutions or laws of most, if not all countries."[98]

The notion of "privacy" as included in the ICCPR was based on a common understanding of what the potential threats to the right would be in

---

92. *See* Barontini & Holden, *supra* note 23, at 11.

93. *See* WORLD BANK *supra* note 24, at 34.

94. *See* Brainard, *supra* note 26, at 8.

95. Schilling, *supra* note 38, at 3.

96. *See* Yanagawa & Yamaoka, *supra* note 1, at 11.

97. General Comment 16, *supra* note 86, ¶ 3.

98. Rep. of the 9th Sess. of the Comm'n on Hum. Rts., ¶ 67 U.N. Doc. E/2447-E/CN.4/689 (June 6, 1953).

1966. Digital currencies were not known in 1966; the concept of a secure digital currency has been theorized only since the 1980s.[99] In the 1960s, the international ratios of physical fiat currency in circulation to nominal GDP was at its peak.[100] Thus, article 17 was drafted in a global economy in which payment privacy was not questioned, as cash provided a widespread way to transact anonymously. Further, there is no mention of payment systems in the ICCPR. While the authors considered the ability to make payments for other purposes,[101] they did not elaborate on any particular right relating to consumer payments or finance. CBDCs do not fall explicitly within the aims or goals of the covenant. A payment system that risks consumer privacy in some forms is at fundamental tension with the understanding of anonymity in payments at the time the framers drafted the covenant.[102] An account-based CBDC is tied to an identity system; from a technological perspective, this eliminates privacy and requires identification of the user.[103] Choosing a system that discards payment privacy, especially in a cashless society, is not consistent with the aims of the covenant.

The second prong of the lawfulness standard requires the action to be pursuant to both domestic and international law. An understanding of the restriction on "unlawful" activities reflects an understanding that an action, even if not arbitrary, must still be envisaged by law.[104] For an action or instrument to be pursuant to both domestic and international law, there must not be a more-narrow, less-intrusive way of reasonably achieving the same

---

99. *See generally* DAVID CHAUM, BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS (1982), http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF (this paper is considered one of the first proposals of a digital currency in history).

100. *See* John Bagnall, David Bounie, Kim P. Huynh, Anneke Kosse, Tobias Schmidt, Scott Schuh, & Helmut Stix, *Consumer Cash Usage: A Cross-Country Comparison with Payment Diary Survey Data*, INT'L J. CENT. BANKING, Dec. 2016, at 1.

101. *See* ICCPR, *supra* note 52, art. 14. ICCPR article 14(d) makes the only statement pertaining to finance or payments within the ICCPR: "Everyone shall be entitled. . . to defend himself in person or through legal assistance of his own choosing. . . to have legal assistance assigned to him, in any case where the interests of justice so require, and without *payment* by him in any such case if he does not have sufficient means to *pay* for it." (emphasis added).

102. Diggelman & Cleis *supra* note 56, at 451 ("In the third committee of the General Assembly, the discussions focused on the relationship between the protection of privacy in general, the family and the home.); *see* Andrea Ryan, Gunnar Trumbull & Peter Tufano, *A Brief Postwar History of U.S. Consumer Finance,* 85 BUS. HIST. REV. 461, 463 (2011) (explaining that even in the U.S., less than a decade before the ICCPR was drafted, "nearly all payment activity. . . was paper based: essentially cash, checks and money orders." This would have been the status quo for the drafters.)

103. Auer & Böehme, *supra* note 20, at 86–87.

104. *See* BYGRAVE, *supra* note 77, at 92 (arguing that under ECHR Article 8(2), commonly read as the affirmative obligations that complement the ICCPR prohibitions, there must be a legal basis for the interference. The legal basis can be statutory, found in rules, or judicially developed).

results available to the government.[105] Further, as shown in *Kononov v. Latvia,* conduct must be analyzed under both the domestic and applicable international law; it cannot be analyzed merely on the more favorable standard.[106]

On a global scale, domestic privacy laws vary widely; much of this discrepancy depends on whether a national society tends towards modern individualism or towards collectivism.[107] Due to the divergence between states, it is beyond the scope of this note to determine whether a CBDC, token-based or account-based, is explicitly permitted by domestic law in each jurisdiction. State entities may not look at protected information directly, but rather monitor, collect, and store mass amounts of personal data indefinitely.[108] Even this moderate approach impacts the privacy of individuals by allowing governments to access significant amounts of data that otherwise would not exist.[109]

On an international scale, the systemic public collection of personal data can fall within the scope of private life protected by article 17 when it "is systemically collected and stored in files held by the authorities."[110] As noted by the Special Rapporteur on the right to privacy, states are risking their compliance with article 17 by implementing new, more invasive technologies.[111] Though account-based CBDCs are likely not explicitly prohibited in domestic legislation, the concept behind the technology would permit the central bank to use an owner register, essentially allowing for full transparency of the amount of money in each account, as well as the amount and recipient of money transfers.[112] A token-based CBDC, while dependent on the technology used in each state, has the potential to allow for peer-to-peer transfers, similar to cash, without the oversight or easily identifiable accounts of a central bank clearing house.[113] Though storing personal data alone does not violate article 17, it does risk running afoul of the European

---

105. *See* ELECTRONIC FRONTIER FOUNDATION ["EFF"], NECESSARY & PROPORTIONATE: INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS LAW TO COMMUNICATIONS SURVEILLANCE 20 (May 2014), https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf.

106. *See* Kononov v. Latvia, App. No. 36376/04, Judgment, Eur. Ct. H.R., ¶¶ 232–244 (2010).

107. *See generally* Gerard Roland & Yuriy Gorodnichenko, *Understanding the Individualism-Collectivism Cleavage and Its Effects: Lessons from Cultural Society, in* INSTITUTIONS AND COMPARATIVE ECONOMIC DEVELOPMENT 213 (Masahiko Aoki, Timur Kuran, & Gerard Roland eds., 2012).

108. *See* EFF, *supra* note 105, at 7.

109. *See id.*

110. *See* Rotaru v. Romania, App. No. 28341/95, Eur. Ct. H.R., ¶ 43, (2000) (also explaining that there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life.").

111. *See* Rep. of the Special Rapporteur on the Right to Privacy, *supra* note 68, ¶ 8.

112. *See* Shirai, *supra* note 49.

113. *See* Terracciano & Somoza, *supra* note 28.

Court of Justice's proposition to give personal financial data the utmost privacy, and the European Court of Human Rights' intention to preserve a private identity in spite of modern technology.[114]

However, the analysis of lawfulness does not end with a simple allowance of infringement by law; rather, the application of the law on the specific instance of infringement on privacy must also be reasonably foreseeable and "detail the precise circumstances in which such interferences may be permitted."[115] Individuals must be able to discern from the language of the law the "circumstances in which and conditions on which public authorities are entitled" to breach the right to privacy.[116] Further, states that are signatories to the ICCPR not only have the responsibility to detail permissible interferences, but also have the affirmative obligation to "undertake the necessary steps to adopt laws or other measures. . . as may be necessary to give effect" to the right to privacy.[117] Currently, mandates permitting the creation of a CBDC are not widespread. As of 2017, roughly twenty-five percent of central banks have the legal authority through their domestic mandates to issue a CBDC, thirty-three percent do not have the legal authority to do so, and the remainder of central banks are unsure as to the legality of an issuance.[118] The widespread lack of certain legal authority presents a large hurdle for central banks; if laws permitting infringement of privacy must detail the precise circumstances in which interferences may be allowed, and financial data should be afforded a high degree of privacy, there must be explicit detailed authorization to infringe on the anonymity of payments. Further, the General Assembly Resolution on the Right to Privacy requires ICCPR signatories to affirmatively shape legislation to protect individuals' rights recognized in the covenant.[119] For the central banks without a current legal mandate to issue a CBDC, any legislation constructing a mandate would have to protect the right to privacy in order to be consistent with the jurisdiction's international obligations. Again, account-based CBDCs, when compared to token-based systems, give rise to less anonymity and less privacy.[120]

---

114. *See* Joined Cases C-293/12, C-594/12, Digit. Rts. Ir. Ltd. v. Minister of Commc'ns, Marine, & Nat. Res. et al., ECLI:EU:C:2014:238 (Apr. 8, 2014); *see also* Malone v. United Kingdom, App. No 8691/79, 1984 Eur. Ct. H.R. (explaining that The Convention protects the community of men; man in our times has a need to preserve his identity, to refuse the total transparency of society, to maintain the privacy of his personality).

115. General Comment 16, *supra* note 86, ¶ 8; *see also* Van Hulst v. Netherlands, U.N. Hum. Rts. Comm. 82d Sess., Commc'n No. 903/1999, ¶¶ 7.3, 7.6, 7.10, U.N. Doc. CCPR/C /82/D/903/1999 (HRC 2004).

116. *See* Taylor-Sabori v. United Kingdom, App. No. 47114/99, Eur. Ct. H.R. 4 (2002).

117. *See* ICCPR, *supra* note 52, art. 2.

118. *See* Barontini & Holden, *supra* note 23, at 12.

119. G.A. Res. 69/166, U.N. Doc. A/RES/69/166, at 4 (Dec. 18, 2014).

120. *See* Terracciano & Somoza, *supra* note 28.

V. THE APPLICATION OF THE ARBITRARY STANDARD TO ACCOUNT-BASED AND TOKEN-BASED CBDCS

A. *Overview of the Standard*

While the lawfulness standard of article 17 does not provide a solidified answer to the question of legality of account-based or token-based CBDCs, the analysis does not end with the "unlawful" provision. Rather, the drafters of the ICCPR included both an unlawful *and* an arbitrariness standard.[121] As anticipated above, the arbitrary standard is often argued to have four prongs, the instrument must: (1) pursue a legitimate aim, (2) have a rational connection to that aim, (3) minimally impair the right to privacy, and (4) strike a fair balance between the pursuit of the aim and the limitation of the right.[122] Further, the introduction of the arbitrariness standard is intended to serve as a limit on the lawfulness standard; conduct that may be acceptable under international and domestic law may still be deemed to infringe on the right to privacy if it does not meet the four factor test.[123] Thus, in addition to being considered lawful, any introduction of a CBDC needs to satisfy all four factors.

B. *Pursuance of a Legitimate Aim*

The CBDC, whether in account-based or token-based form, must be created to pursue a legitimate aim; this factor is easily satisfied in most cases. Generally, emerging market economies have stronger motivations to develop a CBDC compared to advanced economies.[124] However, both types of economies list motivations for creating a CBDC as factors such as financial stability, monetary policy implementation, financial inclusion, domestic payments efficiency, cross-border payments efficiency, and payment safe-

---

121. *See generally* ICCPR, *supra* note 52, art. 17.

122. *See* ACLU, *supra* note 85, at 24. The gist of this four-factor test is widely accepted, but occasionally is phrased differently. For example, in Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 56 (2009), the Inter-American Court held that restrictions on privacy "must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render it necessary in a democratic society." The "statutorily enacted" requirement is directly analogizable to the lawfulness standard, the "legitimate purpose" to the legitimate aim, the "suitability" to the rational connection, the "necessity" to the minimal impairment, and the "proportionality" to the fair balance.

123. *See* General Comment 16, *supra* note 86, ¶ 4; *see also* Van Hulst v. Netherlands, U.N. Hum. Rts. Comm. 82d Sess., Commc'n No. 903/1999, ¶¶ 7.3, 7.6, 7.10, U.N. Doc. CCPR/C/82/D/903/1999 (HRC 2004).

124. *See* CODRUTA BOAR, HENRY HOLDEN, & AMBER WADSWORTH, BANK FOR INT'L SETTLEMENTS, BIS PAPERS NO. 107: IMPENDING ARRIVAL—A SEQUEL TO THE SURVEY ON CENTRAL BANK DIGITAL CURRENCY 1 (Jan. 2019).

ty.[125] Digitization of money has its roots in historical progression; from coins for local commerce to checks for long distance, the evolution of money has been centered around rightful ownership and trust.[126] The evolving form of money is expected to maintain legitimacy and traceable ownership, while at the same time becoming more user-friendly, readily available, safe, and protected against crime and invasion of privacy.[127] The evolution of a CBDC promulgated by a central bank fits into the historical narrative of the expectations of currency, as factors such as payment safety and financial inclusion facilitate a readily available, safe currency; this suggests the aims of creating a CBDC are legitimate under article 17.

C. *Rationally Connected to the Legitimate Aim*

Further, the issuance of both token and account-based CBDCs are rationally connected to the various goals suggested by central banks. CBDC has attracted interest for its proposed ability to address challenges identified by central bankers, such as "financial inclusion, payments efficiency, and payment system operational and cyber resilience."[128] Further, the implementation of a CBDC would provide an instrument to pursue rational policy goals such as anti-money laundering, know your customer, and reduction of tax evasion, though these areas are not frequently the primary goal of the central bank.[129] Both account-based and token-based CBDCs can be created to pursue a legitimate aim, and can be rationally connected to that aim. The first two prongs of the arbitrary standard are not in contention.

D. *Minimal Impairment on the Right to Privacy*

Although CBDCs are not prohibited on the basis of lawfulness or legitimacy alone, the application of the remainder of the arbitrary standard raises

---

125. *Id.* at 4. Most of these factors apply in varying degrees based on the development of the respondent economy. For example, domestic payment efficiency and financial inclusion were rated as "very important" for emerging market economies, whereas payment safety was rated as "very important" for advanced economies. Cross border payment efficiency is the most important for advanced economies researching a wholesale CBDC, but is outside the scope of this note; *see also* BANK OF CANADA, MONETARY AUTH. OF SINGAPORE, AND BANK OF ENGLAND, CROSS-BORDER INTERBANK PAYMENTS AND SETTLEMENTS: EMERGING OPPORTUNITIES FOR DIGITAL TRANSFORMATION (2019).

126. *See* Lagarde, *supra* note 3, at 2.

127. *Id.*

128. WORLD ECON. F. ["WEF"], CENTRAL BANKS AND DISTRIBUTED LEDGER TECHNOLOGY: HOW ARE CENTRAL BANKS EXPLORING BLOCKCHAIN TODAY? 4 (2019); *but see* WALTER ENGERT & BEN S.C. FLUNG, BANK OF CANADA, CENTRAL BANK DIGITAL CURRENCY: MOTIVATIONS AND IMPLICATION (2017) (where increasing competition in payments and financial stability are considered to be sound motivations for issuing a CBDC, financial inclusion can be legitimate reasoning, but reducing effective lower bound on interest rates and inhibiting criminal activity are not legitimate aims for issuance).

129. *See* WEF, *supra* note 128, at 9.

the largest, and potentially detrimental, hurdles for account-based CBDCs, especially in a cashless society. Prong three of the arbitrary interference test requires states to choose the infringement that has minimal impairment on privacy. An account-based CBDC would not "minimally impair" the right to privacy because the centralized structure requires reliance on the central bank to act as the central node. The use of a central node amplifies the amount of information a state could access and would minimize the amount of privacy a consumer would be able to choose.[130] The imposition of a minimal impairment standard implies that encroachment on privacy must not be merely useful to the state, but rather there is a direct and immediate nexus between the legitimate aim and the remedy suggested.[131] Further, even actions taken in accordance with a legitimate aim can be found to violate international privacy guidelines when there is no adequate guarantee against abuse.[132] While there are a wide variety of approaches to issuance of a CBDC, it is possible to use distributed ledger technology ("DLT") in a token-based system to settle peer to peer transactions, eliminating the need for a central record-keeper.[133] Using DLT in this way could enable central banks to issue a token-based CBDC that would not require central bank interference for settlement. A token-based system would limit the amount of information available to the government when compared to the account-based system, and act similarly to the role of cash. Because of the availability of a less intrusive alternative, an account-based system likely does not satisfy the minimal impairment standard.

While state actors benefit from a wide scope of deference to the means chosen for achieving the legitimate aim, deference will not be given to every instance of impairment.[134] CBDCs present a clear occasion of multiple discrete forms of infringement achieving similar results, with strikingly different privacy implications. In a token-based system, user A could send the CBDC from their wallet, through a decentralized system, to user B's wallet.[135] Many systems utilizing DLT rely on the identification of the token being transferred as legitimate, rather than rely on the identification of the

130. Schilling, *supra* note 38, at 3.

131. *See* Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, No. 16-7081 (D.C. Cir., Nov. 1, 2016).

132. *See* Weber & Saravia v. Germany, App. No. 54934/00, Decision on Admissibility, Eur. Ct. H. R., ¶ 106 (June 29, 2006).

133. *See* CPMI, *supra* note 19, at 8.

134. *See generally Weber*, App. No. 54934/00 *supra* note 132, ¶ 80 (interferences must not only have a legitimate aim, but must also be justified, and be necessary in a democratic society in order to achieve those aims).

135. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 8 (however, the ledger where the token is sent could also be centralized, and thus lack the anonymity in the described example).

sender or recipient.[136] These systems are similar to cash, in that the transfer of value is decentralized and does not require a central clearing party.[137] In contrast, in an account-based system, the payor must be identified as the proper owner of the account from which the transaction is being sent.[138] The distinction between these two systems is one of central bank control and amount of anonymity. The account-based system could permit the central bank to view all transactions of account holders, whereas the token-based system can be designed to mitigate these privacy concerns.[139]

Further, even if a central bank were to consider the minimal impairment standard, central banks would have no individual incentives to issue a CBDC that would transfer anonymously with validation by distributed ledger technology.[140] Doing so would weaken their role as a regulator or supervisory body.[141] The current proposals for CBDC are generally not for media that circulates anonymously peer-to-peer, but rather for a central clearing system.[142] A leading cryptocurrency critic, Roubini, acknowledges that the currency central banks are envisaging issuance of would rely on a centralized system, with a single ledger, available to every individual in the economy, thereby avoiding any situation with private transactions.[143] This system could dominate not only cash deposits, but also alternative payment systems such as PayPal or Square, because the rational consumer would not pay even a small fee for payment transfer services provided by the central bank for free.[144] In effect, the central bank's ability to enhance their own role in the payment infrastructure by creating a system where all payments go

---

136. Charles Kahn, Francisco Rivadeneyra & Tsz-Nga Wong, *Should the Central Bank Issue e-Money?* (Working Paper 2019-003A, January 2019), https://pdfs.semanticscholar.org/6475/78020ed229bdce9ee5a3a12d4c1d85b15c6d.pdf.

137. *See id.* at 3–4.

138. *Id.* at 8.

139. Schilling, *supra* note 38, at 3.

140. Nouriel Roubini, Keynote Speech at BEF Davos: Fintech Revolution Coming, Nothing To Do With Blockchain (Feb. 1, 2019), https://www.youtube.com/watch?v=97keNLmxP0c.

141. *See generally* Tobias Adrian & Tommaso Mancini-Griffoli, *Central Bank Digital Currencies: 4 Questions and Answers,* IMFBLOG (Dec. 12, 2019), https://blogs.imf.org/2019/12/12/central-bank-digital-currencies-4-questions-and-answers/ (a central bank that choses to issue a CBDC would be responsible for "potentially including interfacing with customers, building front-end wallets, picking and maintaining technology, monitoring transactions, and being responsible for anti-money laundering and countering the financing of terrorism." A CBDC that transfers anonymously would be more difficult to monitor, leading to potential reputational risk.).

142. *See* Lawrence White, *Efficient "Central Bank Digital Currency" is a Fantasy,* CATO INST., (Feb. 11, 2019), https://www.cato.org/blog/efficient-central-bank-digital-currency-fantasy.

143. *See* Roubini, *supra* note 140.

144. *See id.* (on an international scale, this critique would apply to systems such as Alipay in China, M-Pesa in Kenya, and so on).

through a central bank clearinghouse could squeeze out more anonymous payment systems. The elimination of more anonymous payment systems would minimally impair the right to privacy.

Past examples of regulatory abuse showcase why an account-based CBDC in a cashless society could be disastrous for the international right to privacy. For example, in the United States, the Federal Deposit Insurance Corporation worked to decline banking services to lawfully operating businesses such as payday lenders.[145] In order to accomplish this goal, the government agencies had to pressure banks to cut off banking relationships with the targeted companies.[146] Crucially, paper notes remained an option for doing business if the legal entity was denied a bank account.[147] However, if this regulatory abuse reoccurred in a cashless economy, the regulators could make it impossible for legal businesses to process payments as there would be no anonymous alternative. Instead of relying on pressuring private entities, the authorities could directly monitor and shut down retail accounts,[148] halting any access to currency.[149] The least restrictive measure to protect a legitimate aim should not have the potential to stunt various industries, leading to potential collapses of entire businesses.[150] Account-based CBDCs un-

145. For a deeper understanding of Operation Choke Point, *see* Nobert Michel, *Newly Unsealed Documents Show Top FDIC Officials Running Operation Choke Point,* FORBES, (Nov. 5, 2018, 6:30 PM), https://www.forbes.com/sites/norbertmichel/2018/11/05/newly-unsealed-documents-show-top-fdic-officials-running-operation-choke-point/#640a8f721191. The FDIC targeted businesses that "have been understood by industry and financial regulators as being subject to complex or varying legal and regulatory environments (such as activities that may be legal only in certain states); being prohibited for certain consumers (such as minors); being subject to varying state and federal licensing and reporting regimes; or tending to display a higher incidence of consumer complaints, returns, or chargebacks." FED. DEPOSIT INS. CORP. OFF. OF AUDITS & EVALUATIONS, REPORT NO. AUD 15-008 THE FDIC'S ROLE IN OPERATION CHOKE POINT AND SUPERVISORY APPROACH TO INSTITUTIONS THAT CONDUCTED BUSINESS WITH MERCHANTS ASSOCIATED WITH HIGH-RISK ACTIVITIES 2–3 (2015).

146. *See* Dennis Shaul, *There's No Downplaying the Impact of Operation Choke Point,* AM. BANKER (Nov. 28, 2018, 10:39 AM), https://www.americanbanker.com/opinion/theres-no-downplaying-the-impact-of-operation-choke-point.

147. The availability of an anonymous source of transactions remains important for legal business on a statewide scale, such as the Marijuana Banking Sector. *See* MICHAEL S. BARR, HOWELL E. JACKSON, & MARGARET E. TAHYAR, FINANCIAL REGULATION: LAW AND POLICY 182 (2d ed., 2017).

148. *See* CENT. BANK DIGIT. CURRENCIES WORKING GRP., KEY ASPECTS AROUND CENTRAL BANK DIGITAL CURRENCIES POLICY 19 (2019) (explaining the potential for regulatory abuse by authorities, "central banks could be called upon to provide CBDC users' data to tax and other authorities (e.g. for judicial matters)").

149. I would like to thank Professor Lawrence H. White for his insights and guidance on this paper, specifically as it relates to Operation Choke Point.

150. *See* Ben Emmerson, Special Rapporteur, *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/69/397, ¶ 18 (Sept. 23, 2014) (promulgating the least intrusive principle, which holds the "measure chosen be the least intrusive instrument among those which might achieve the desired result.").

dertaken in a cashless society would be privy to this type of abuse without guaranteeing adequate safeguards, and thus would impair the right to privacy.[151]

E. *Proportionality of the Pursuit of the Aim and the Limitation of the Right*

Finally, any potential infringement promulgated by the state must be analyzed under a proportionality test, comparing the balance between the pursuit of an aim and the limitation of the right. When any restriction is made that infringes on a fundamental right, states must only undertake efforts that "are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights [. . .]. In no case may the restrictions be applied or invoked in a manner that would *impair the essence* of a covenant right."[152] For states that pursue a CBDC as an alternative to cash as physical currency use dwindles or becomes unavailable due to exigent circumstances, the argument to proportionally limit privacy may exist, as having some form of currency is necessary for individuals to make transactions. However, states that adopt a CBDC for alternate reasons, such as preference for less cash or better compliance with countering-the-financing-of-terrorism ("CFT") regulations, are likely in violation of the proportionality standard of article 17.

Countries that face a bona fide currency access crisis may have more demanding, legitimate state aims in issuing a CBDC;[153] these higher stakes aims may allow slightly more limitation on the right to privacy but never a complete limitation.[154] For example, in states such as the Republic of Marshall Islands, where the population risks being cut off from the financial system completely due to geographic and economic constraints,[155] the need for some widely accessible form of currency is apparent. However, any form of currency must not only serve a permissible purpose, but also allow for the maximum amount of privacy to be maintained.[156] Although currency presents a special consideration of bulk collection of personal transaction data, an individual must have a method of purchasing power to be an active participant in the economy. Concerns have already been raised about the

---

151. *See* Weber & Saravia v. Germany, App. No. 54934/00, Decision on Admissibility, Eur. Ct. H. R., ¶ 106 (June 29, 2006).

152. Off. of the High Comm'r for Hum. Rts., General Comment No. 31, the Nature of the General Legal Obligation Imposed on State Parties to the Covenant, ¶ 6, U.N. Doc. 31CCPR/C/21/Rev.1/Add.13, (May 26, 2004) (emphasis added) [hereinafter General Comment 31].

153. *See* Ye & Desouza, *supra* note 36.

154. *See* Emmerson, *supra* note 150, ¶ 19.

155. IMF, *Republic of the Marshall Islands: Selected Issues*, IMF Country Rep. No. 18 /271, at 3, 10 (2018) (explaining that while some do not agree the SOV is a CBDC, it is not disputed that access to traditional banking is minimal).

156. *See* General Comment 31, *supra* note 152, ¶¶ 11–16.

ability of the state to access data in the first place, and subsequently share it among different parts of the state.[157] Should states eliminate physical fiat currency and issue a CBDC, governments would have unparalleled access to financial transactions, bypassing the first concern of access to the data. Thus, the risk of violating the proportionality constraint in this instance is striking: While populations undeniably need currency for reasons such as financial inclusion, the anonymity offered by cash is vital in maintaining the least invasive solution to the right to privacy. In jurisdictions where access to cash is threatened, CBDCs may be a viable solution.[158] However, in order to comply with both the least intrusive instrument and proportionality standards, states must adopt CBDCs that do not completely demolish anonymity in payments.

Alternatively, other states are motivated to promulgate a CBDC due to an unwanted "high reliance on cash. . . and improving know-your-customer and countering-the-financing-of-terrorism ("KYC"/"CFT") arrangements."[159] This motivation ultimately violates international privacy law if the CBDC does not have privacy safeguards and is issued in lieu of cash. States are permitted to infringe on the article 17 right to privacy for certain legitimate aims. However, the former special rapporteur explicitly affirmed that "countering terrorism is not a trump card which automatically legitimates interferences with the right to privacy."[160] The policy goals of enhancing KYC and CFT are a microcosm of the classical tradeoffs in record-keeping systems between access, privacy, and security.[161] Issuing a CBDC represents an attempt at achieving perfect security, inevitably sacrificing consumer privacy. The tradeoff between access and privacy is analogizable to the type of system being utilized.[162] Proponents of issuing a CBDC for KYC or CFT purposes tend to rely on the model of an account-based currency.[163] However, the account-based system requires the central clearing party to verify each transaction,[164] leading to mass surveillance of every transfer. In a system without an option for receiver verification (i.e., without token-based digital currencies), utilizing a CBDC to increase KYC or CFT policy goals represents a disproportionate infringement of privacy.

---

157. Fred H. Cate, James X. Dempsey & Ira S. Rubenstein*, Systemic Government Access to Private-Sector Data*, 2 INT'L DATA PRIVACY L. 198 (2012).

158. *See generally* IMF, *supra* note 155 (discussing the issue of access to cash).

159. *See* BOAR ET AL., *supra* note 124, at 4.

160. Martin Scheinin, Special Rapporteur, *The Promotion and Protection of Human Rights and Fundamental Freedoms with Countering Terrorism,* ¶ 13 U.N. Doc A/HRC/13/37 (2009).

161. *See generally* Kahn et al., *supra* note 136, at 9.

162. *See generally id.*

163. *See generally* SRIRAM DARBHA & RAKESH ARORA, BANK OF CANADA, PRIVACY IN CBDC TECHNOLOGY*,* STAFF ANALYTICAL NOTE 2020-09 (June 2020).

164. *See* Kahn et al., *supra* note 136, at 9.

Ultimately, due to the least restrictive infringement principle and the requirement that any infringement be proportionate, the use of an account-based CBDC in a cashless society is in violation of international privacy law. While infringing on privacy through the promulgation of CBDCs cannot be summarily condemned,[165] the existence of anonymous means of payment provides a critical channel for individuals to choose to protect their digital life from mass data collection. Additionally, the existence of a token-based CBDC, where tokens can be verified by the recipient rather than a central clearing house, suggests that account-based CBDCs are not the least restrictive infringement on privacy in many, if not all, cases. Finally, while certain policy aims may be regarded as lawful and legitimate, the complete mass interference with privacy in payments strongly suggests a disproportionate outcome.

PART V: POLICY IMPLICATIONS

The token-based model, discussed throughout the paper, can prevail on privacy concerns when designed to maintain anonymity in payments.[166] Unfortunately for the implementation of CBDC technology, decentralized tokens will cost a magnitude more than alternate models.[167] Many central banks are in the investigative stage and do not plan to immediately issue a CBDC;[168] this delayed timeline suggests that a potential solution to avoid violating international privacy laws is to wait until the decentralized token technology is widespread and developed enough to offset the greater cost of verification. By delaying the introduction of a CBDC model, states may be able to avoid having to make the choice between privacy, security, and access.

Further, if states choose to pursue a CBDC, central banks should recognize the fundamental tension between international privacy laws and central bank incentives. Central banks may lack incentive, besides compliance with international privacy laws, to issue a digital currency that would be validated by a distributed ledger system and circulate anonymously.[169] Due to this lack of incentive, central banks should take specific note of the balance of the pursuit of the aim and the limitation on the right to privacy and cautiously approach CBDCs with the goal of preserving access to anonymous payment methods. Importantly, individual consumers value anonymity in cur-

165. *See* Emmerson, *supra* note 150, ¶ 7 (reasoning that an assessment of the legality and proportionality of surveillance measures must be undertaken using a case by case basis).

166. *See* MANCINI-GRIFFOLI ET AL., *supra* note 6, at 11.

167. *See* Sarah Allen, James Grimmelmann, Ari Juels, & Eswar Prasad, *Design Choices for Central Bank Digital Currency*, BROOKINGS (July 23, 2020), https://www.brookings.edu/blog/up-front/2020/07/23/design-choices-for-central-bank-digital-currency/ (explaining that while there are cryptographic systems to maintain privacy, they are complex and costly).

168. *See generally* Barontini & Holden, *supra* note 23, at 7–8.

169. *See* White, *supra* note 142.

rency.[170] Previous attempts to digitize payments on a state to individual basis have already raised many concerns in states such as Australia and represent the extension of government regulation into personal autonomy and private life.[171]

PART VI: CONCLUDING THOUGHTS

As technology progresses, central banks are not only presented with more options on how to pursue currency, but also must consider the best options in light of international standards protecting the right to privacy.[172] Article 17 of the ICCPR creates an external limit on the innovation of CBDCs, as Central Banks themselves may not have an incentive to pursue the most anonymous form of currency. Article 17 imposes two umbrella standards to consider for any potential infringement of privacy: lawfulness and arbitrariness. The four-part test to determine whether an infringement on privacy is lawful is: (1) consistency with the covenant, (2) pursuant to domestic and international law, (3) accessibility, and (4) clearly defined. The four-part test to determine whether an infringement on privacy is arbitrary is: (1) pursuance of a legitimate aim, (2) rational connection to the legitimate aim, (3) minimal impairment to the right of privacy, and (4) proportionality between the pursuit of the legitimate aim and the limitation of the right to privacy.

Proposed CBDCs should be analyzed under article 17 because of the sensitive nature of the mass aggregation of financial data. In particular, states that are moving towards a cashless society, whether involuntarily or voluntarily, must not eliminate the ability to transact and make payments anonymously. Central banks that choose to experiment with CBDCs should ensure that their currencies are lawful and not arbitrary. Crucially, under the arbitrary infringement analysis, the CBDC must minimally impair privacy and must not infringe on privacy more than they pursue a legitimate policy goal. All aspects considered of both the arbitrary and lawfulness tests, token-based CBDCs present the option for a more anonymous alternative to physical fiat payment when compared to the account-based CBDC alternative. Though the anonymity of cash is difficult to replicate, a token-based system provides for a peer-to-peer transfer system that does not require the approval or aggregation of personal financial data in a central clearinghouse. Ultimately, the account-based CBDC violates international privacy standards due to the development of the token-based alternative that inherently intrudes less on the right to privacy.

---

170. *See supra* Borgonovo et al, *supra* note 16, at 28.

171. *See generally* Michael Edwards, *Move to Cash-Free Economy Comes with Concerns Over Privacy, Cybercrime, Expert Warns,* ABCNEWS (Mar. 27, 2017), https://www.abc.net.au/news/2017-03-28/how-much-privacy-will-you-lose-in-a-cashless-society/8390460.

172. *See generally* Allen et al., *supra* note 167.