Volume **3** (1) 2021 https://doi.org/10.5204/lthj.1745

Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency

Ellie Rennie
Blockchain Innovation Hub, RMIT University, Australia
Stacey Steele
Melbourne Law School, The University of Melbourne, Australia

Abstract

The economic fallout of the COVID-19 pandemic prompted many governments to provide emergency payments to citizens. These one-off and recurring payments revealed the shortcomings of existing financial infrastructures even as electronic payments replaced cash for everyday expenses. Delays in getting government payments to citizens in many countries focused attention on the potential benefits of central bank digital currencies (CBDCs). This article outlines the social and economic policy choices involved in designing a CBDC and the consequences of these choices for privacy. Priorities including preventing the criminal abuse of the financial system, geopolitical concerns and private sector innovation compete with, and potentially undermine, privacy. We identify and categorize four key privacy risks as 'losses' associated with current CBDC models: loss of anonymity, loss of liberty, loss of individual control, and loss of regulatory control.

***Keywords**:* CBDC; Central Bank Digital Currency; privacy; data protection; pandemic; COVID-19.

Introduction: Emergency Payments in a Pandemic

As businesses closed and people retreated indoors during the early months of the COVID-19 crisis, nation states found themselves confronted by the inadequacies of their own financial infrastructures. By 11 June 2020, three months after the World Health Organization declared a global pandemic, 131 countries around the world had committed to direct cash transfers to assist people through the crisis.[1] Governments deployed existing systems including tax records and social security infrastructure to identify recipients and transfer payments, but these proved to be slow processes. The challenges of administering emergency cash transfers during COVID-19 accelerated interest in digital currencies. For example, lawmakers in the United States (US) put forward three proposals for the creation of digital wallets or a new digital dollar for the purpose of COVID payments.[2] These proposals were intended to provide a means for the Federal Reserve to pay citizens and businesses directly.

At the beginning of the pandemic, discussions of central bank digital currencies (CBDCs) were nascent, but emerging. A survey of central banks by the Bank for International Settlements (BIS) in late 2019 found that 10% were likely to issue a CBDC for the general public in the short term, representing 20% of the world's population.[3] Eighty per cent of the banks had undertaken conceptual work on digital currencies, 40% had progressed to experiments or proofs of concept, and another 10% had developed pilot projects.[4]

[1] Gentilini, Social Protection.
[2] *Automatic Boost to Communities Act*, H.R 6553, 116th Cong. (2019–2020); *Financial Protections and Assistance for America's Consumers, States, Businesses, and Vulnerable Populations Act*, H.R 6321, 116th Cong. (2019–2020); *Take Responsibility for Workers and Families Act*, H.R. 6379, 116th Cong. (2019–2020).
[3] Boar, Impending Arrival.
[4] Boar, Impending Arrival, 3.

Yet, concerns about privacy were—and remain—a key obstacle to the successful deployment of digital currencies.[5] This article considers the meaning of privacy in the context of developing a credible CBDC that might accelerate payments during any future emergency.[6] Many reports on CBDCs mention the issue of privacy, but do not go on to articulate these perceived risks.[7] As this article demonstrates, CBDCs have the potential to diminish individual privacy, whether defined as freedom from intrusion into private life or the ability of an individual to control her or his own personal information and protect against its misuse, or with reference to data protection, security and safety, or even freedom from mass monitoring, profiling or surveillance.[8] Moreover, we suggest that the design for a CBDC will be inextricably linked to the understanding of risks based on a broad conceptualization of privacy.

This article first examines the use of existing electronic payments mechanisms during the pandemic and highlights how these differ from proposed CBDCs. Next, we categorize the different models of CBDCs emerging globally and the benefits a CBDC might offer in a future emergency. We then identify the types of privacy concerns created by CBDCs, which we argue reflect debates about privacy in existing electronic payment systems but are amplified by the scale of CBDCs. CBDCs provide a case study for what Richardson might describe as stretching traditional concepts and expectations of privacy to help address complex future problems.[9] Adopting this approach, we 'stretch' concerns about CBDCs and privacy to include the potential for the abuse of power by states or other authorities traditionally identified with the concept of 'data protection,' which we categorize in this article as a 'loss of regulatory control.' We also identify sometimes competing goals for a CBDC that help us to start thinking about responses to these privacy concerns in the context of an emergency such as a pandemic. Depending on which of these goals are prioritized by the relevant jurisdiction, we predict different outcomes for user privacy. We suggest that being clear about the goals for any CBDC will help central banks to explain choices that will need to be made about the level of privacy offered by a particular CBDC. We recognize that these choices may differ depending on the goals of each jurisdiction.

The Use of Electronic Payments in a Pandemic

A large proportion of everyday financial transactions already consist of information transmitted across digital infrastructure rather than the exchange of physical cash.[10] CBDCs received attention during the pandemic on the basis that they might speed up payments by giving governments a direct payment channel to recipients. In the US's response to the COVID crisis, some people received support through pre-loaded electronic cards that could be transferred into a bank account or used anywhere that accepts Visa.[11] Others used Venmo or PayPal to receive payments.[12] While these commercial systems likely eased the difficulty in accessing entitlements for some, they also exposed the fragilities and interdependencies within the payments system. The US media reported that some payments stalled because relief checks relied on a software programming language that had not been widely used in decades.[13] Bermuda undertook 'stimulus token' pilots after finding that issuing payments was a 'very cumbersome process.'[14]

To unpack how CBDCs could be of benefit in a pandemic, we need to first consider the key differences between central bank money and commercial banking and payment processes. Digital payment systems that dominate consumer transactions involve private sector entities carrying out identity processes and administering accounts on behalf of customers. These systems then provide consumers with the *experience* of instant digital payment systems and other financial services, including credit services, but they are not cash. Cash is money that is issued by a central bank. Cards and electronic transfers do not use central bank money but rather commercial bank money—a liability that private sector financial institutions hold to the central bank

[5] Bank of England, Central Bank Digital Currency, 32; Bank of Canada, Central Bank Digital Currencies, 6; Expert Group on Regulatory Obstacles to Financial Innovation, 30 Recommendations. The European Commission's Expert Group on Regulatory Obstacles to Financial Innovation identified the General Data Protection Regulation (Regulation [EU] 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation [GDPR]) as an obstacle to new applications of technology and called on the European Data Protection Board to provide more guidance on the innovative use of technology in financial services (see Recommendation 25)—especially distributed ledger technology/blockchain and how to satisfy the requirement for erasure, encryption and artificial intelligence, and specificity of consent.

[6] The European Parliamentary Research Service (EPRS) calls for a 'data strategy,' which incorporates concepts of cyber-resilience, compliance with GDPR and addressing concerns about data storage, and notes that more specific guidance for the financial sector is required when it comes to the application of GDPR as a general matter. See Saulnier, Digital Finance.

[7] For example, see Bank of England, Central Bank Digital Currency; World Economic Forum, Central Banks.

[8] Richardson, Advanced Privacy Law, chaps 1–2.

[9] Richardson, Advanced Privacy Law, 4, 11–12, 25.

[10] Swartz, New Money.

[11] Consumer Financial Protection Bureau, "EIP Debit Cards."

[12] Kelley, Testimony.

[13] Long, "Stimulus Checks."

[14] Casey, "Bermuda."

(responsible for money supply, interest rates and other policy instruments). The commercial bank or authorized financial provider will convert this electronic IOU into cash at a customer's command and honour customer payments, as long as it has sufficient balances to do so. Within this highly regulated system, technologies such as card payment networks interact with base technological infrastructures that are maintained by central banks and intergovernmental organizations. What we currently think of as payments are, therefore, more like instructions—messages between financial providers to update their records to reflect an exchange. CBDCs may streamline government payments by potentially eliminating the commercial bank IOU and sending the equivalent of cash direct.

CBDCs and Potential Payments Benefits in a Pandemic

COVID-19 coincided with advances in digital technology, including cryptocurrency, that are demonstrating alternative methods for stable, instant and trusted payments. A cryptocurrency is issued only in digital form and can be held by the owner and stored in a software or hardware wallet without the need for a financial services provider.[15] Cryptocurrencies such as bitcoin were designed for peer-to-peer exchange. They may be described as 'money,' because they are a ledger of account and a store of value.[16] The blockchains that are used for cryptocurrencies can also be used for other purposes, providing infrastructure for applications to run where exchange of value is required and replacing some of the roles of institutions by overcoming trust problems.[17]

CBDCs are digital currencies where the party issuing and redeeming the currency is a central bank. Unlike cryptocurrencies built using blockchain technology, these do not necessarily use distributed ledgers, but they do rely on an electronic ledger that is updated whenever a transaction occurs. One of the most advanced projects is China's Digital Currency/Electronic Payment (DC/EP, also known as the digital RMB), developed by the research arm of the People's Bank of China (PBC) and already piloted in four large cities.[18] We group the key emerging models of CBDCs into three broad categories: direct digital banknotes, platform CBDC, and synthetic CBDC.

Direct Digital Banknotes. In designing a CBDC, a central bank may opt for a system in which 'regular savers are granted accounts with the Federal Reserve so the government can frictionlessly remit them new digital dollars,'[19] effectively creating a retail arm between central banks and the public. The benefit of this model for consumers is that digital money would be like cash in its peer-to-peer usability. This model would offer convenient real-time payments, be widely accessible, may not require credit checks (because it does not involve providing credit), and provide easy cross-border payments.[20] China's DC/EP falls between this model and the platform model (below): the DC/EP is issued by the PBC, with state-owned commercial banks developing wallets for consumers to use the currency.

Platform CBDC. The Bank of England has proposed a 'platform model,' whereby the bank would provide a core ledger, which would record CBDC and process payments.[21] Private sector 'payment interface providers' would be licensed to provide customer-facing services and to access the application programming interface of the central bank ledger. These providers would be the intermediary between the user and the ledger, performing 'know your customer' identity checks, and gathering anti-money laundering and sanctions information. The private sector would issue customer accounts. In 2020, Sweden's Riksbank commenced a pilot of an e-krona structured so that the central bank issues e-krona to participating banks, which then distribute the e-krona to end users.[22]

Synthetic CBDC. A third model sees the private financial services industry given even greater scope to create services and products through what is called a synthetic CBDC. In this scenario, a government would licence financial service providers who would store their customers' funds in a central bank account. The company then receives a central bank liability in return that they could 'package' as a stablecoin, fully backed by the central bank reserves.[23] Multiple private companies could issue

[15] Bank of England, Central Bank Digital Currency, 7–8.
[16] Dodd, "The Social Life of Bitcoin," 35–56. Some reject the analysis of cryptocurrencies as money because, for example, they are considered too volatile and not widely accepted. See Bank of England, Central Bank Digital Currency, 9. However, not all cryptocurrencies are volatile. For example, Dai maintains a relatively stable peg to the US dollar.
[17] Blockchain ledgers update across a network of participants, using algorithms and economic incentives to arrive at social consensus that an event or exchange has occurred. Therefore, blockchains overcome the need for intermediaries to oversee records or verify accounts. Hayes, "Socio-Technological Lives"; Berg, Understanding the Blockchain Economy.
[18] Xiao, "China to Expand Testing."
[19] Carter, "Après Le Déluge," para. 5.
[20] Auer, "Central Bank Digital Currency," 86.
[21] Bank of England, Central Bank Digital Currency, 25–32.
[22] Sveriges Riksbank, E-krona Pilot. See also Sveriges Riksbank, E-krona Project.
[23] Mancini-Griffoli, The Rise of Digital Money.

their own stablecoins (all backed by the same CBDC) and compete with one another by offering different attributes, such as tokens that provide businesses with the ability to pay employees with interest-bearing stablecoins.[24] A group of central banks together with the BIS argued that this model of stablecoin is not a CBDC, as the user does not hold a claim on the central bank and because the provider could not expand its balance sheet when demand required.[25] Experience in Bermuda, which does not have a central bank, suggests that something akin to a CBDC may be achieved by licensing private cryptocurrency stablecoins, including for government tax and services, and providing for a claim against the government itself.[26] For the purposes of this article we consider the synthetic CBDC alongside the direct and platform models, because the regulatory framework would still require that the funds be matched by the central bank or other state-based organizations.

Central banks are not 'designed to manage spending.'[27] Instead, they were designed to 'issue currency, provide liquidity to the government bond market, and mitigate banking panics.'[28] Therefore, the first of these models represents a shift towards central banks becoming more like a retail provider, whereas the other two models maintain a system in which private, accredited companies are the interface with consumers. While issuing citizens with accounts at a central bank may be effective for distributing emergency payments or welfare, some central banks are reluctant to directly administer such goods and services for the public.[29] The Bank of England makes a case against the first model:

> This approach does not play to the [Bank of England's] comparative advantage, as it involves building services for large numbers of retail customers rather than for financial institutions. Building user-friendly services for the general public is a strength of the UK private sector, which can also build on this experience to ensure they provide inclusive services.[30]

In a Reserve Bank of New Zealand bulletin, Wadsworth also pointed out that this approach could reduce resilience in the private banking sector as '[c]ommercial banks might find they lose some deposits as households put money into a central bank digital currency.'[31]

In the context of the pandemic, it was not up to the central banks to facilitate payments per se, but there was an accelerated understanding of the potential benefits of CBDCs, including the possibility that central banks could play a more direct role in the future. The successful use of cryptocurrencies in the humanitarian sector during the pandemic also underscored the potential.[32] Key advantages highlighted by the pandemic include resilience and efficiencies in interbank transfers, preventing money laundering and terrorism, and increasing financial inclusion.

Since CBDCs could be cash-like in their usability, including merchants receiving money instantly rather than waiting for batched card payments or incurring the risk of later chargebacks, they could reduce costs associated with payment and credit providers. If commercial banking infrastructure fails or if there were a run on the bank—as is more likely to occur in a time of crisis—a CBDC system could provide people with access to their money directly (assuming digital connectivity was maintained). International payments to overseas crisis-affected areas, including donations and remittances, may also be easier with digital currencies. Remittance payments currently incur costs related to cross-border payments, as outlined by the G7, in the form of 'correspondent banking fees, FX costs, telecommunication costs, scheme fees and interchange fees. Additionally, legal, regulatory and compliance costs are perceived as being significantly higher than for domestic retail payments.'[33] These could be dramatically reduced or eliminated with digital currencies.

CBDCs might assist those who are already excluded from commercial banking to access emergency payments: this is estimated at one billion people worldwide, including 14 million adults in the US.[34] However, platform and synthetic models of CBDCs could reproduce existing bank and payment provider barriers for those who do not have legal identity documents or are excluded due to bank fees. The extent to which digital exclusion would need to be resolved for those currently excluded from commercial banking services to benefit from a CBDC has so far been glossed over in the CBDC debate. The World Economic Forum notes

[24] Kulechov, "Permissionless."
[25] Bank of Canada, Central Bank Digital Currency, 4.
[26] Klein, "Bermuda."
[27] Blyth, "Print Less," 98–109.
[28] Blyth, "Print Less," 98–109.
[29] Labonte, Financial Innovation, 2.
[30] Bank of England, Central Bank Digital Currency, 24.
[31] Wadsworth, "Pros and Cons," 15.
[32] Helms, "UNICEF Funding."
[33] G7 Working Group on Stablecoins, Global Stablecoins, 4.
[34] Apaam, Unbanked and Underbanked Households.

that 'policy-makers must seek to encourage the unbanked to participate in any new digital currency regime. They must be aware of hurdles to adoption such as usability challenges, access, or insufficient government identity documentation.'[35]

CBDCs could also be used for payments, including micropayments, within automated systems. A smart contract is 'a contract-like arrangement expressed in code, where the behavior of the program enforces the terms of the contract.'[36] A CBDC could be programmable, designed for transferring value on internet-of-things platforms, energy grids, government services, taxation and myriad other uses. China has been piloting a national blockchain called the Blockchain-based Service Network, with which the DC/EP will likely interoperate.[37] This network is intended for use with supply chains (the digital silk road), smart cities and government services. In the emergency context, payments administered through the tax system through smart contracts could potentially provide nuanced levels of support—for example, if governments wanted to ensure that workers affected by the pandemic receive benefits relative to their usual income.[38]

Privacy and CBDCs: What Are the Key Risks and Concerns?

Despite the potential benefits offered by CBDCs in times of crisis, governments are considering competing needs in designing a CBDC, especially effects on expectations of 'privacy.' The Bank of Canada calls for a whole-of-society approach to determining the acceptable 'trade-offs and risks':

> Privacy is not the sole purview of the Bank, and we will need to clarify the exact level of privacy to consider by consulting with external institutions (e.g., the Privacy Commissioner of Canada, civil liberties advocates, law enforcement and the Financial Transactions and Reports Analysis Centre of Canada).[39]

The Bank of Canada's call for an interdisciplinary approach demonstrates a broad conceptualization of privacy. The Bank of England notes that both privacy and data protection 'should be considered carefully when designing CBDC,' offering users 'control over how their data is used and who it is shared with.'[40] The Bank's use of both 'privacy' and 'data protection' in its 2020 report suggests an understanding of how these issues may differ in connection with a CBDC and reflects different jurisdictional approaches and terminology in this field. The Bank of Canada report only mentions 'data protection' once, whereas there are numerous references to concerns about 'privacy.'[41]

Considerations of 'privacy' in the context of CBDCs extend beyond a traditional notion of freedom from intrusion into private lives seen as 'fundamental to human dignity and flourishing,' and encompass concerns traditionally embodied in the concept of 'data protection,' such as control over personal information and resisting surveillance. We also see the meaning of privacy in connection with CBDCs as extending to perceived threats to human dignity and control emanating from artificial intelligence and automation.[42]

The potential loss of privacy in connection with the emergence of CBDCs and their use in emergencies plays into overarching concerns that the pandemic is being exploited to entrench systems that erode privacy. We categorize the key privacy risks as four 'losses' associated with the current categories of CBDC models to help frame these discussions: loss of anonymity, loss of liberty, loss of individual control, and loss of regulatory control. Conceptualizing privacy as 'losses' helps to clarify the issues and move the debate towards a risk-based analysis whereby central banks can begin to address privacy concerns associated with CBDCs, rather than the issues being perceived as a series of 'trade-offs' that suggests privacy is something with which to be bargained.[43]

Loss of anonymity is closely associated with traditional concepts of privacy that resist intrusion, and loss of liberty encompasses the potential for increased exposure to surveillance and monitoring. Loss of individual control over personal information aligns with contemporary ideas of data protection, including protecting information from misuse, such as through unauthorized commercialization, and freedom from automatic decision-making. The final category of loss of 'regulatory control' starts to address geopolitical rivalries and position individuals vis-à-vis the emerging battle for leadership in the global financial sector inherent in China's challenge of the US and Europe. The identification of privacy risks under a category of 'loss of regulatory

[35] World Economic Forum, Central Banks, 9.
[36] Sills, "Smart Contracts," para. 1.
[37] Reggianini, DLT Solutions, 50.
[38] Tillett, "Pay Rise for Part-Timers."
[39] Shah, "Technology Approach."
[40] Bank of England, Central Bank Digital Currency, 31.
[41] Darbha, "Privacy in CBDC Technology."
[42] Richardson, Advanced Privacy Law, 3, 25. Richardson traces the history of two distinct rights to privacy and data protection.
[43] Compare the use of a 'trade-off' framework in Bank of Canada, Central Bank Digital Currency, 16.

control' stretches the concept of 'privacy' to reflect a growing literature that seeks to advance traditional notions of privacy, as well as data protection, to encapsulate these broader, emerging concerns.[44]

First, loss of anonymity refers to the reduction in freedoms that are more likely to be prevalent in the use of physical cash than CBDCs. Physical cash offers much greater privacy than any of the categories of CBDCs identified in this article. However, limits on these freedoms already exist, such as where jurisdictions and circumstances allow sellers to refuse cash, and sophisticated ways of tracking withdrawals and deposits that prevent anonymity, which may have historically been attached to cash.[45] The increased use of electronic payments has also already substantially reduced the privacy effect of physical cash. Moreover, the Bank of England argued in its CBDC framing paper that:

> the appropriate degree of anonymity in a CBDC system is a political and social question, rather than a narrow technical question. … Some discussions of CBDC assume that CBDC is equivalent to cash and so should offer the same degree of anonymity in payments. … The Bank does not have a specific mandate to provide untraceable or anonymous payment methods.[46]

The Bank's stated objective for CBDC payments is to provide households and businesses with a 'fast, efficient and reliable' payment mechanism, which is 'inclusive, innovative, competitive and resilient.'[47] Efficiency is also prioritized in a report published by a group of central banks with the BIS, which notes that CBDC infrastructure would need to process a large number of payments at once, possibly requiring 'compromises' to features such as 'computationally demanding privacy techniques.'[48]

The loss of anonymity is closely related to the second loss we identify as a 'loss of liberty.' This concept is a reference to the potential for increased surveillance by authorities based on the data collection inherently involved in CBDCs. While cash is hard to trace, the Library of Congress notes:

> a CBDC that provided complete anonymity would seemingly be incompatible with current policies designed to curb money laundering and other illicit activities. Thus, the Fed may be required to track and store information about CBDC users and their transactions. This would reduce individuals' privacy, but might be more effective at preventing illicit activity.[49]

One of the appeals of a direct CBDC for governments is that it could make it easier to combat money laundering and terrorism financing, and to enforce sanctions.[50] CBDCs potentially increase the capacity for state surveillance compared to cash. Governments could also coerce citizens and firms by stopping payments. The more centralized the platform, the more likely that the system administrator—that is, the central bank—will also be required to enforce privacy policy.[51] This result means that the organization with the most access to the data is also the organization enforcing society's expectations when it comes to privacy—with potentially varying consequences for levels of surveillance—whether or not they seek that role.

A third privacy concern associated with CBDCs is a 'loss of individual control' over an individual's own personal information. Transactions involving CBDCs have the potential to generate user data ripe for commercialization or other tracking and big data analytics. When combined with artificial intelligence, these trends have implications for price discrimination and financial inclusion and equality.[52] These concerns have already emerged in payment systems and loyalty card programs that have the ability to track individuals and feed into general commercial surveillance models prevalent in the private sector. These issues are also linked to debates over data ownership.[53]

A fourth concern that we identify from a privacy perspective is a potential 'loss of regulatory control.' This concept is inherent in the potential for personal information associated with CBDCs to cross international boundaries and emerging geopolitical conflicts over the control and transfer of data. The prospect of individuals in one jurisdiction being the subject of surveillance of another jurisdiction that controls the CBDC means that privacy protections may not be equal to those offered in the

[44] Richardson, Advanced Privacy Law, chaps 1–2.
[45] The Australian Transaction Reports and Analysis Centre is an Australian Government agency 'for preventing, detecting and responding to criminal abuse of the financial system to protect the community from serious and organised crime.' See https://www.austrac.gov.au/about-us/austrac-overview
[46] Bank of England, Central Bank Digital Currency, 32.
[47] Bank of England, Central Bank Digital Currency, 20.
[48] Bank of Canada, Central Bank Digital Currencies, 15.
[49] Labonte, Financial Innovation, 2.
[50] Bank of Canada, "Contingency Planning."
[51] Bank of Canada, Central Bank Digital Currencies, 14, Table 2.
[52] EPRS notes that insurance markets are a particular concern when it comes to the potential for digital developments to exclude certain segments of society. See Saulnier, Digital Finance, 16.
[53] Gensler, "Facebook Cryptocurrency," 3.

jurisdictions where the individual resides.[54] The Court of Justice of the European Union's Schrems II decision on July 2020, which invalidated the EU–US Privacy Shield, called into question transfers of personal data from the European Union to the US, revealing the fragility of international understandings about data flows.[55] A loss of regulatory control means that CBDCs also have the potential to undermine existing political hegemonies and frameworks, including the Chinese Communist Party or European democracy, in a way that involves a loss of privacy based on the processing of big data. The concern regarding concentration of user data generated by any particular CBDC in the hands of a particular central bank—and, thus, jurisdiction—also harks back to the impetus for the establishment of general data protection laws at a national level in Europe in the 1970s, and concerns that existing national legislation was insufficient to protect privacy rights as against automated data banks.[56]

Emerging economies may also be pressured to accept development loans using the preferred CBDC of the donor country, and CBDCs have the potential to undermine the effect of sanctions and to hamper the ability of authorities to track illicit financial flows.[57] The vast majority of international payments are currently managed through the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Information sharing between SWIFT and corresponding banks means that authorities can track illicit payments such as money laundering and terrorist financing. Countries that are excluded from SWIFT cannot pay for imports or receive payments for exports. Russia, China and the European Union have created alternatives, and by creating CBDCs countries might avoid the gaze of international agreements and conventions.[58] Venezuela's petro, reportedly backed by state-owned oil and mineral reserves, was developed at least partly to support sanctions circumvention, as was Iran's plan to issue a state-backed 'crypto-rial' currency.[59]

'Loss of regulatory control' is inextricably linked to an expanded concept of privacy in the context of CBDCs because they create data in ways that can be used to reduce freedoms for whole communities. The advent of a globally significant CBDC has serious implications for the ability of any domestic regulator, including data protection authorities, to regulate the processing of user data and enforce applicable laws.[60] Regulatory focus on cloud computing and data storage already demonstrates the concerns of financial services regulators about the storage of data outside traditional territorial divides, and they also have implications for how CBDCs are developed to preserve this emerging conceptualization of privacy.

Can CBDC Design Provide for Privacy-Enabling Solutions?

How much privacy is 'lost' with the introduction of CBDCs will depend on what model is implemented—a classic case study of so-called privacy by design where privacy-enhancing tools may be built into the technology supported by technology-neutral regulation. Existing payment mechanisms, including cash, are not 'privacy perfect' in any event.

Support for privacy in the regulation of existing payment systems may have potential application to CBDCs to minimize any loss of anonymity and liberty. One straightforward privacy-enhancing solution is for central banks to commit to the continued issuance of cash as a viable alternative to CBDCs. Even if parties such as consumers and retailers avoid using or accepting cash, as experienced during the pandemic, maintaining choice for individuals supports privacy outcomes. The approach of the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's financial crimes regulator, is also instructive. Domestic fund transfers are a key source of intelligence and they are mostly distributed in data silos sitting across the financial system. AUSTRAC receive information on domestic fund transfers through a 'suspicious matter report' where the reporting entity questions the legitimacy of a domestic transaction, or if a transaction is above AUD$10,000 in cash or 'e-currency.'[61] To address transactions that fall below this threshold, AUSTRAC worked with members of the Fintel Alliance, a public–private partnership established by AUSTRAC, to develop data-matching and machine-learning tools that are combined with privacy-preserving technology.[62] This is used to identify and surface financial crime risks that do not become visible until they join up disparate and distributed data silos in a privacy-preserving manner.[63] Once a case for suspicion has been established, AUSTRAC can then request that the banks provide the identities of those involved, and commence further manual investigation, which may lead to law enforcement activities.

[54] The individual may choose not to use the CBDC of another jurisdiction, but for some services or goods the individual may have no practical alternative.
[55] *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18, 'Schrems II').
[56] Coppel, Information Rights, 131.
[57] Kumar, "China's Digital Currency."
[58] Blakstad, FinTech Revolution, 109.
[59] World Economic Forum, Central Banks, 12.
[60] Some commentators call for enhanced privacy and data protection laws as a result of the emergence of CBDCs. See Hoffman, Flipside of China.
[61] *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), pt 3.
[62] Privacy-preserving technologies, such as homomorphic encryption, allow for encrypted data to be used without decrypting it first.
[63] Kee Siong Ng, interviewed by Ellie Rennie, 29 August 2018.

Somewhat similarly, the Bank of England's platform model means that customer accounts, issued by the approved financial services provider, could remain pseudonymous on the core ledger, providing some level of assurance against state surveillance. These requirements can be enforced through privacy-enhancing technologies/techniques known as 'PETs.'[64] Rules could also be established such that public and private entities would need the consent of the user or an independent third party such as a court before collecting or accessing financial data; however, there are limits to the efficacy of this approach.

Authors in English-language literature on CBDCs tend to assume a democratic setting. Researchers at the Massachusetts Institute of Technology believe that cryptographic techniques could be used to maintain a level of privacy, arguing that, 'legitimate public policy goals relating to combating criminal activity can be fulfilled while preserving the privacy of the public and preventing a central bank being drawn into the commercial surveillance models which are now prevalent in the private sector.'[65] They suggest that development of such systems could perhaps best be done in collaboration with institutions that are democratically accountable and already regulate currency.[66] However, the privacy concerns we identify go further than commercial surveillance models. Moreover, the status of central banks is not without controversy. Central banks have been criticized as lacking democratic accountability where commissioners are not elected and a bank's mandates themselves call for independence from parliaments.[67]

The ultimate solution will require a combination of regulatory and cryptographic techniques to provide privacy assurances that may not yet be obvious. CBDCs may not use blockchain or distributed ledger technology (DLT), for example. The Head of Payments Policy at the Reserve Bank of Australia, Richards, highlighted the potential 'negative aspects' of DLT when it comes to privacy and performance, because 'each update of the ledger must be shared between nodes operating on the network, with the nodes coming to agreement on the state of the ledger through a consensus mechanism.'[68] The visibility of transactions on public blockchains could be mitigated by a permissioned DLT. According to Richards, such a DLT should have 'access limited to payment service providers or other regulated entities' and 'a consensus mechanism' for settlement 'with some degree of centralisation.'[69]

Under the synthetic model described above, an entity such as Diem (formerly the Libra Association), established by Facebook, could be authorized to provide a stablecoin for use on their own and other platforms. A scenario in which multiple, privately issued stablecoins exist, approved and regulated by government authorities, interacting with revamped central bank infrastructure, raises the issue of how personal data is used within multifaceted platforms. Stablecoins would extend the existing data-network-activities loop, or 'DNA' loop, of 'big tech' platforms,[70] amplifying their ability to triangulate and use consumer data. Privacy may be supported in this context by establishing and enforcing a specification of purpose model that prohibits the further commercialization of personal data collected in connection with the CBDC, similar to the restrictions called for in relation to COVID-19-related health data. Individual rights to sue for misuse of information and consumer-driven lawsuits for misleading and deceptive conduct may also help to reinforce these restrictions. Finally, the dominance of data collection and analysis has prompted calls for a radical reconceptualization of information privacy law.[71] CBDCs represent a moment in time in which governments will have to 'work hard to produce limited zones of privacy.'[72]

The loss of regulatory control may be the most difficult privacy concern to comprehend and overcome in the context of a CBDC. Some surveillance scholars may even argue that this whole category of concerns might be better dealt with outside a privacy framework.[73] The COVID-19 pandemic has demonstrated differing levels of tolerance for incursions into privacy by the state in different jurisdictions.[74] In China, the DC/EP will come with a centralized governance structure under the control of the PBC and, while privacy is to be protected within the private sector, it seems likely that the government will have access to data.[75] Even among members of the Organisation for Economic Co-operation and Development, there is no consensus when it comes to acceptable levels of data protection, as demonstrated by the Schrems II decision and lack of adequacy decisions

[64] European Central Bank, Balancing Confidentiality and Auditability, 1.
[65] Ali, Redesigning Digital Money, 11.
[66] Ali, Redesigning Digital Money, 13.
[67] Best, "Accountability in Uncertain Times."
[68] Richards, Retail Central Bank Digital Currency, 6. Some privacy-oriented public blockchains are finding ways to do private transactions.
[69] Richards, Retail Central Bank Digital Currency, 6.
[70] Gensler, "Facebook Cryptocurrency," 3.
[71] Burdon, Digital Data Collection, 257–288.
[72] Richardson, Advanced Privacy Law, 62, quoting William J. Mitchell.
[73] Richardson, Advanced Privacy Law, 23–25.
[74] For example, see Nortes, "Generation App."
[75] Arner, After Libra, 38; Hoffman, Flipside of China.

from the European Commission under the General Data Protection Regulation.[76] Similarly, the local sociopolitical environment and attitudes to privacy are likely to dictate the level of acceptance of a CBDC in any particular jurisdiction.

CBDCs will also need to operate on platforms that enable them to be exchanged for other currencies.[77] Even without this interoperability it is possible that a CBDC of one nation could gain widespread adoption in another, similar to the US dollar being accepted in some foreign countries. Financial sovereignty vis-à-vis private actors is also a key driver behind the development of CBDCs and underpins concerns about a loss of regulatory control.[78]

Conclusion

COVID-19 revealed the deficiencies in existing payment systems during an emergency and resulted in increasing contactless payments. However, solutions such as CBDCs are yet to fully address concerns surrounding user privacy. Anonymity akin to cash is unlikely for users of CBDCs when other factors are considered, including anti-money laundering. Depending on the model chosen by the relevant central bank, the private sector may also play an important role in the development and implementation of a CBDC. The extent to which CBDCs provide companies and governments with visibility over consumer transactions in ways that are not visible through cash, or at least not so concentrated through existing electronic payment systems, is, therefore, a key issue. As the Bank of England noted, privacy equivalence to that achievable through existing payment systems is unlikely when it comes to CBDCs. However, there are ways in which the loss of privacy associated with CBDCs may be mitigated, potentially providing greater levels of privacy than existing commercial payment systems. The categorization of the different ways in which a CBDC may lead to a loss of privacy helps to provide a framework for analyzing and resolving these concerns.

Acknowledgements

The authors thank the reviewers for their helpful comments and Dr Geraldine Carney, University of Melbourne, and Mr Campbell McNolty, RMIT University, for their research assistance. Professor Ellie Rennie is the recipient of an Australian Research Council Future Fellowship (FT190100372), funded by the Australian Government. This article reflects the authors' personal opinions. Statements do not represent the views or policies of the authors' employers, past or present, or any other organization with which the authors are affiliated.

Bibliography

Ali, Robleh and Neha Narula. *Redesigning Digital Money: What Can We Learn from a Decade of Digital Currencies?* (MIT Digital Currency Initiative, 2020). https://dci.mit.edu/research/2020/1/22/redesigning-digital-money-what-can-we-learn-from-a-decade-of-cryptocurrencies-by-robleh-ali-and-neha-narula-of-the-digital-currency-inititaive

Apaam, Gerald, Susan Burhouse, Karyen Chu, Keith Ernst, Kathryn Fritzdixon, Ryan Goodstein, Alicia Lloro, Charles Opoku, Yazmin Osaki, Dhruv Sharma and Jeffrey Weinstein. *National Survey of Unbanked and Underbanked Households* (Federal Deposit Insurance Corporation, 2017). https://www.fdic.gov/householdsurvey/2017/2017report.pdf?mod=article_inline

Arner, Douglas W., Ross P. Buckley, Dirk Andreas Zetzsche and Anton N. Didenko. *After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems. European Banking Institute Working Paper Series 65/2020; University of Hong Kong Faculty of Law Research Paper No. 2020/036* (University of Hong Kong/European Banking Institute, 2020). http://doi.org/10.2139/ssrn.3622311

Auer, Raphael and Rainer Böhme. "The Technology of Retail Central Bank Digital Currency." *BIS Quarterly Review* (2020): 85–100.

Australian Transaction Reports and Analysis Centre. "Regulation." Last updated December 11, 2019. https://www.austrac.gov.au/about-us/regulation

Bank of Canada. "Contingency Planning for a Central Bank Digital Currency." February 25, 2020. https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency

[76] *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18, 'Schrems II').
[77] Giancarlo, Digital Dollar Project, 8.
[78] Sweden's e-krona stems from concerns that hegemony by private payment markets could undermine trust in the integrity of the national monetary system, erode competitiveness and stability, and exclude certain groups of people. See Sveriges Riksbank, E-krona Project, 2.

Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, and Bank for International Settlements. *Central Bank Digital Currency: Foundational Principles and Core Features. CBDC Report No. 1* (Bank for International Settlements, 2020). https://www.bis.org/publ/othp33.pdf

Bank of England. *Central Bank Digital Currency: Opportunities, Challenges and Design* (Bank of England, 2020). https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

Berg, Chris, Sinclair Davidson and Jason Potts. *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*. Cheltenham: Edward Elgar, 2019.

Best, Jacqueline. "Rethinking Central Bank Accountability in Uncertain Times." *Ethics & International Affairs* 30, no 2 (2016): 215–232. https://doi.org/10.1017/S0892679416000095

Blakstad, Sophie and Robert Allen. *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*. Cham: Palgrave Macmillan, 2018.

Blyth, Mark and Eric Lonergan, "Print Less but Transfer More: Why Central Banks Should Give Money Directly to the People." *Foreign Affairs* 93, no 5 (2014): 98–109.

Boar, Codruta, Henry Holden and Amber Wadsworth. *Impending Arrival: A Sequel to the Survey on Central Bank Digital Currency. BIS Papers No 107* (Bank for International Settlements, 2020). https://www.bis.org/publ/bppdf/bispap107.pdf

Burdon, Mark. *Digital Data Collection and Privacy Law*. Cambridge: Cambridge University Press, 2020.

Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press, 2014.

Carter, Nic. "Après Le Déluge, Bitcoin." *The American Mind*, April 30, 2020. https://americanmind.org/features/online-money-money-online/apres-le-deluge-bitcoin/

Casey, Michael J and Sheila Warren. "Bermuda Will Skip the Age of CBDCs, with Premier David Burt." Produced by CoinDesk. *Money Reimagined*, October 30, 2020. Podcast, 52:01. https://www.coindesk.com/podcasts/late-confirmation/bermuda-david-burt-age-cbdcs

Consumer Financial Protection Bureau. "Economic Impact Payment (EIP) Prepaid Debit Cards." https://www.consumerfinance.gov/coronavirus/managing-your-finances/economic-impact-payment-prepaid-debit-cards/

Coppel, Philip. *Information Rights: A Practitioner's Guide to Data Protection, Freedom of Information and Other Information Rights*. London: Bloomsbury, 2020.

Darbha, Sriram and Rakesh Arora. "Privacy in CBDC Technology." Analytical Note 2020-9. *Bank of Canada*, June 2020. https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/#Tradeoffs-and-risks

Dodd, Nigel. "The Social Life of Bitcoin." *Theory, Culture & Society* 35, no 3 (2018): 35–56. https://doi.org/10.1177/0263276417746464

European Central Bank and Bank of Japan. *Balancing Confidentiality and Auditability in a Distributed Ledger Environment* (European Central Bank and Bank of Japan, 2020). https://www.boj.or.jp/announcements/release_2020/data/rel200212a1.pdf

Expert Group on Regulatory Obstacles to Financial Innovation. *30 Recommendations on Regulation, Innovation and Finance* (European Commission, 2019). https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

G7 Working Group on Stablecoins. *Investigating the Impact of Global Stablecoins*. *CPMI Papers No. 187* (Bank for International Settlements, 2019). https://www.bis.org/cpmi/publ/d187.pdf

Gensler, Gary. "Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System." Testimony to the Financial Services Committee, United States House of Representatives, 17 July 2019. *MIT Media Lab*, June 18, 2019. https://www.media.mit.edu/posts/examining-facebook-s-proposed-cryptocurrency-and-its-impact-on-consumers-investors-and-the-american-financial-system/

Gentilini, Ugo, Mohamed Almenfi and Pamela Dale. *Social Protection and Jobs Responses to COVID-19: A Real-Time Review of Country Measures* (World Bank Group, 2020). https://socialprotection.org/discover/publications/social-protection-and-jobs-responses-covid-19-real-time-review-country

Giancarlo, Charles H., J. Christopher Giancarlo, Daniel Gorfine and David B. Treat. *Digital Dollar Project: Exploring a US CBDC* (Digital Dollar Foundation, 2020).

Hayes, Adam. "The Socio-Technological Lives of Bitcoin." *Theory, Culture & Society* 36, no 4 (2019): 49–72. https://doi.org/10.1177/0263276419826218

Helms, Kevin. "UNICEF Funding Startups with Cryptocurrency for COVID-19 Relief." *Bitcoin*, June 21, 2020. https://news.bitcoin.com/unicef-funding-cryptocurrency/

Hoffman, Samantha, John Garnaut, Kalya Izenman, Matthew Johnson, Alexandra Pascoe, Fergus Ryan and Elise Thomas. *The Flipside of China's Central Bank Digital Currency*. *Policy Brief Report No. 40/2020* (Australian Strategic Policy Institute, International Cyber Policy Centre, 2020). https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency

Kelley, Jodie. *Testimony Before the House Financial Services Committee Task Force on Financial Technology Hearing on Inclusive Banking During a Pandemic Using FedAccounts and Digital Tools to Improve Delivery of Stimulus* (US House Committee on Financial Services, 11 June 2020). https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-kelleyj-20200611-u1.pdf

Klein, Michael. "Bermuda to Accept Digital Currency." *Cayman Compass*, October 17, 2019. https://www.caymancompass.com/2019/10/17/bermuda-to-accept-digital-currency/

Kulechov, Stani. "Permissionless Building with Aave." Digital ETHGlobal DeFi Summit, October 16, 2020. https://ethonline.org/defi/

Kumar, Aditi and Eric Rosenbach. "Could China's Digital Currency Unseat the Dollar?" *Foreign Affairs*, May 20, 2020. https://www.foreignaffairs.com/articles/china/2020-05-20/could-chinas-digital-currency-unseat-dollar

Labonte, Marc, Rebecca M. Nelson and David W. Perkins. *Financial Innovation: Central Bank Digital Currencies*. *Report No. IF11471* (Congressional Research Service, 2020).

Long, Heather, Jeff Stein, Lisa Rein and Tony Romm. "Stimulus Checks and Other Coronavirus Relief Hindered by Dated Technology and Rocky Government Rollout." *The Washington Post*, April 18, 2020. https://www.washingtonpost.com/business/2020/04/17/stimulus-unemployment-checks-delays-government-delays/

Mancini-Griffoli, Tommaso and Tobias Adrian. *The Rise of Digital Money*. *FinTech Notes No. 2019/001* (International Monetary Fund, 2019). https://www.imf.org/-/media/Files/Publications/FTN063/2019/English/FTNEA2019001.ashx

Nortes, Silvia, Laura Silvia Battaglia and Steven Borowiec. "Generation App: How Do Different Generations Feel about Sharing Personal Data in Order to Tackle COVID-19? We Ask People in South Korea, Spain and Italy." *Index on Censorship* 49, no 2 (2020): 18–23. https://doi.org/10.1177/0306422020935791

Reggianini, Eugenio. *DLT Solutions for Trade and Finance: China Focus* (Hyperledger Trade Finance Special Interest Group and Hyperledger Capital Markets Special Interest Group, 2020). https://wiki.hyperledger.org/display/TFSIG/DLT+solutions+for+trade+and+finance+-+China+Focus

Richards, Tony. "Retail Central Bank Digital Currency: Design Considerations and Rationales." UWA Blockchain, Cryptocurrency and Fintech Conference, October 14, 2020. https://www.rba.gov.au/speeches/2020/pdf/sp-so-2020-10-14.pdf

Richardson, Megan. *Advanced Introduction to Privacy Law*. Cheltenham: Edward Elgar, 2020.

Saulnier, Jérôme and Ilaria Giustacchini. *Digital Finance: Emerging Risks in Crypto-Assets. Regulatory and Supervisory Challenges in the Area of Financial Services, Institutions and Markets* (European Parliamentary Research Services, 2020). https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654177

Shah, Dinesh, Rakesh Arora, Han Du, Sriram Darbha, John Miedema and Cyrus Minwalla. "Technology Approach for a CBDC." Analytical Note 2020-6. *Bank of Canada*, February 2020. https://www.banqueducanada.ca/2020/02/note-analytique-personnel-2020-6/

Sills, Kate. "Smart Contracts." *Libertarianism.org*, December 16, 2019. https://www.libertarianism.org/topics/smart-contracts

Sveriges Riksbank. *The Riksbank's E-krona Pilot* (Sveriges Riksbank, 2020). https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf

———. *The Sveriges Riksbank's E-krona Project: Report 2* (Sveriges Riksbank, 2018). https://www.riksbank.se/en-gb/payments--cash/e-krona/e-krona-reports/e-krona-project-report-2/

Swartz, Lana. *New Money: How Payment Became Social Media*. New Haven: Yale University Press, 2020.

Tillett, Andrew and David Marin-Guzman. " 'Pay Rise' for Part-Timers Raises Doubt over Fairness of Wage Subsidy." *Financial Review*, March 31, 2020. https://www.afr.com/politics/federal/pay-rise-for-part-timers-raises-doubts-over-fairness-of-wage-subsidy-20200331-p54flp

Wadsworth, Amber. "The Pros and Cons of Issuing a Central Bank Digital Currency." *Reserve Bank of New Zealand Bulletin* 81, no 7 (2018): 3–21.

World Economic Forum. *Central Banks and Distributed Ledger Technology: How Are Central Banks Exploring Blockchain Today?* (World Economic Forum, 2019). http://www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf

Xiao, Eva. "China to Expand Testing of a Digital Currency." *Wall Street Journal*, August 14, 2020. https://www.wsj.com/articles/china-to-expand-testing-of-a-digital-currency-11597385324

Primary Legal Material

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

Automatic Boost to Communities Act, H.R. 6553, 116th Cong (2019–2020).

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18: 'Schrems II').

Financial Protections and Assistance for America's Consumers, States, Businesses, and Vulnerable Populations Act, H.R. 6321, 116th Cong (2019–2020).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Take Responsibility for Workers and Families Act, H.R. 6379, 116th Cong (2019–2020).