Reserve Bank of New Zealand
Te Pūtea Matua

Designing privacy into digital cash

Digital Cash Consultation Note #4

17 April 2024

Disclaimer

We produce a variety of publications and research about monetary policy, financial stability and related economic and financial issues. Most are available without charge as part of our public information service.

We have made every effort to ensure that information published in this paper is accurate and up to date. However, we take no responsibility and accept no liability arising from:

- errors or omissions
- the way in which any information is interpreted
- reliance upon any material.

We are not responsible for the contents or reliability of any linked websites and do not necessarily endorse the views expressed within them.

Privacy Policy - Reserve Bank of New Zealand - Te Pūtea Matua (rbnz.govt.nz)

Contents

Authors: Bella Di Mattina-Beven and Amber Wadsworth[1]

1 The authors are grateful to the Office of the Privacy Commission, the RBNZ CBDC External Forum, Dr Marcin Betkier, Tim Duston, Damian Henry, Matteo Solinas, Robbie Taylor, and Evelyn Truong for their comments. Any errors presented in this article are the authors' own.

Abstract

New Zealanders care about the privacy of their transactions. They describe their privacy concerns in different ways, including the freedom to choose when and how they spend their money. This was evident in the submissions to the Reserve Bank of New Zealand's 2021 Future of Money Issues Papers. It is clear that digital cash in New Zealand must be private. However, defining what privacy means can be challenging. The New Zealand legal system continues to grapple with the meaning of privacy, along with sociologists, technologists and economists. This note investigates public and academic views on the dimensions of privacy relevant to digital cash. It finds that digital cash must go beyond protecting personal information to be private. Digital cash must also provide for contextual privacy needs. This means upholding New Zealanders right to live freely and be in control of their identity, choices and actions. It also means designing for te ao Māori views of privacy that include collective information ownership and Māori data sovereignty.

1 Introduction

The Reserve Bank of New Zealand (Reserve Bank) is exploring issuing digital cash.[2] This exploration takes place in a changing landscape for payments, where the Reserve Bank's goal is to enable reliable and efficient money and payment systems supporting innovation and inclusion. Global attention has been given to the demand for better, smarter, and faster forms of payments, while access to, and use of, physical cash is declining.

The Reserve Bank first raised the prospect of exploring issuing digital cash in the Future of Money – Central Bank Digital Currency (CBDC) Issues Paper in 2021 ('2021 Issues Paper'). We received over 6000 responses to the issues paper, with many bringing up issues of privacy, control, and personal freedom. Respondents referred to concepts of privacy in different ways.

This note aims to unpack what people mean when they talk privacy and to use that to inform the design of a privacy-centric digital cash. It sets out a broad description of the concept of privacy and develops privacy design recommendations for digital cash. The findings in this note support the Digital cash in New Zealand Consultation Paper.

The rest of this note is set out as follows. Section two introduces a privacy ontology for New Zealand that centres on two forms of privacy: information and contextual privacy. Section three expands on the components of information and contextual privacy and explains the relationships between the two. Section four applies this broader view of privacy to develop a 'Privacy' principle for digital cash and makes design recommendations. Section five acknowledges the constraints on a privacy-centric digital cash and section six concludes.

2 Introducing a privacy ontology for New Zealand

There is no simple definition of privacy. Privacy concerns can span from data collection and use to government control and the ability to live one's life freely. Raymond Wacks in the Poverty of Privacy says, "Privacy has grown into a large and unwieldy concept".[3] Other legal theorists and sociologists agree that privacy is difficult to define, and thus difficult to legally enforce.[4] Finally, Alan Westin, in the Social and Political Dimensions of Privacy notes that the digital world may require a different approach to privacy protection.[5]

2.1 New Zealand privacy legislation and sentiment

There is no single definition of privacy in New Zealand law and no statutory right to it. The Bill of Rights Act 1990 explicitly excluded a right to privacy because the "boundaries would be uncertain and contentious".[6] Instead, the Bill of Rights Act 1990 contains implied rights to particular aspects of privacy such as property rights; the right to freedom of thought, conscience and religion; the right to freedom of association; the right not to be subjected to medical or scientific experimentation; and the right to refuse to undergo medical treatment.[7]

The Privacy Act 2020 aims to "promote and protect individual privacy" but focuses only on personal information privacy. It protects personal information from being collected, used, or

2 Previous consultation referred to this as a general-purpose central bank digital currency.
3 (1980).
4 See, e.g. Mulligan et. al (2016); and Westin (2003).
5 Westin (2003).
6 Liddicoat (2017).
7 Kim (2019).

shared in a way that harms New Zealanders by setting out the obligations on agencies that collect personal information. Its principles derive from the Organisation for Economic Co-operation and Development (OECD) Guidelines that attempt to harmonise data protection internationally. It was updated in 2020 to reflect changing privacy needs in an increasingly digital economy. Other New Zealand legislation protect certain aspects of privacy in a piecemeal manner.[8] Common law also does not recognise a right to privacy although there are protections given by certain case law.

Despite the shortcomings in legal protections, New Zealanders care about privacy, and these feelings are heightened in an increasingly digitised world.[9] A digital identity survey in New Zealand found that 73 percent of respondents claim to have changed their online behaviour because of privacy concerns. These fears were echoed in some of the submissions to our 2021 Future of Money consultation.[10] The word 'privacy' was included in 1764 out of 5848 responses to the 2021 Issues Paper. The respondents expressed varied approaches to privacy, associating it with data protection, surveillance, control, freedom, and dignity:

- "The meta data around transactions within the context of a digital currency, creates unlimited opportunities for governments to leverage that data and exert control"
- "Cyber security and privacy breaches are of massive concern and such events destroy trust in organisations"

2.2 The two broad components of privacy

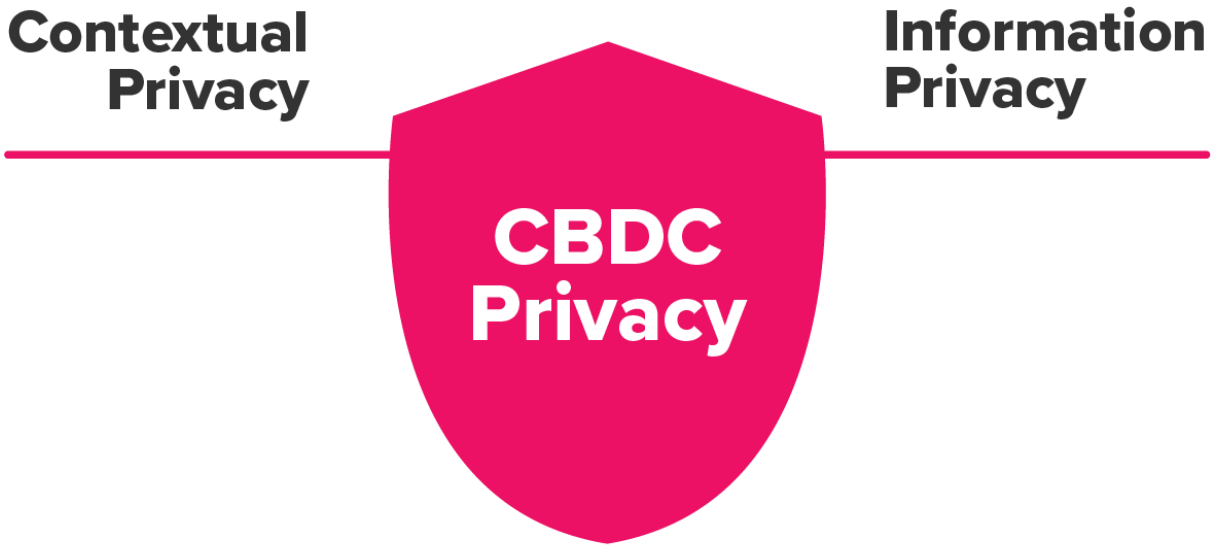
We find there are two broad components of privacy: information privacy and contextual privacy. These are not entirely separate and share some common elements. In fact, all privacy could be considered contextual. However, it is worth splitting out information privacy as its own category as this is where the majority of New Zealand legal protections lie.

8 Broadcasting Act 1989; Crimes Act 1961, ss 216H (criminalises intimate visual recordings of another person) and 216B (criminalises use of interception device to capture another person's private communications); Harassment Act 1997 (bodily privacy); Harmful Digital Communications Act 2015; Residential Tenancies Act 1986, s 38 (spatial privacy); and Search and Surveillance Act 2012 as summarised by Kim (2019).

9 The New Zealand Crime and Victims Survey released June 2023 reported that deception and fraud offences (including credit card fraud) have increased in recent years – increasing to 510 000 in 2022 (10 percent of adults) from 288 000 in 2021 (6 percent of adults). See NZCVS Cycle 5 (November 2021 – November 2022).

10 rbnz.govt.nz/money-and-cash/future-of-money.

Figure 1: Information and contextual privacy



Source: Reserve Bank.

Information privacy

Information privacy concerns typically relate to the governance and rules around the collection, use, sharing, correction, and deletion of information. This is a somewhat narrow definition of privacy but useful to distinguish what many people initially think of when they consider privacy.

Information privacy is of clear concern to New Zealand.

- Just over half of the respondents to the Privacy Commissioner's 2020 Privacy Concerns survey were concerned about individual privacy and the protection of personal information, and these concerns had increased for 52 percent of respondents over the last few years. The potential for businesses to share personal information without permission was the largest area of concern (75 percent of respondents).[11]
- The BNZ Digital Skills Report[12] found 78 percent of respondents were concerned about entering personal details online, up from 73 percent in 2021.
- Many respondents to the 2021 Issues Paper had privacy concerns regarding the digital nature of digital cash transactions and the potential for their information to be collected and used.

Concern regarding information privacy is not surprising. Personal, physical and transaction information are easily collected and shared through digital applications such as customer loyalty programmes, social sharing sites, and messaging applications.

Privacy is also contextual

Concerns about privacy also span to feelings of safety, trust, autonomy and being in control. This note uses the concept of 'contextual privacy' to capture these broader feelings. These include

11 Office of the Privacy Commissioner (2020a).
12 BNZ (2021)

feeling 'free from harm' due to the misuse or sharing of your information and feeling 'free to control' what information you reveal, who holds it, how it is used and more. The term 'contextual privacy' comes from the research of sociologists that considered privacy as part of an individual's sense of freedom and control, affecting their human dignity.[13] Westin's four functions of privacy including personal autonomy, emotional release, self-evaluation, and limited and protected communication.[14]

Contextual privacy in New Zealand also includes Māori views. Māori views on privacy reflect tikanga Māori (loosely translated as practices, values, knowledge, cultures, and customs) and experiences of how information has historically been used in a way that impacts them. There are precedents in case law where tikanga Māori has been an influencing consideration with respect to privacy, specifically in Te Pou Matakana Limited v Attorney-General.[15]

The Privacy Act 2020 does not address people's contextual privacy concerns, and it also does not fully address all information privacy concerns. For example, although the Privacy Act 2020 protects personal information privacy, it does not give people agency and control over their information. In fact, the Privacy Act 2020 only gives people a right to request an agency to delete information, but it falls short from giving people the right for their information to be deleted.

The wide range of privacy concerns raised by New Zealand's could be partly due to the imperfect privacy protection afforded by the the Bill of Rights Act 1990 and Privacy Act 2020.

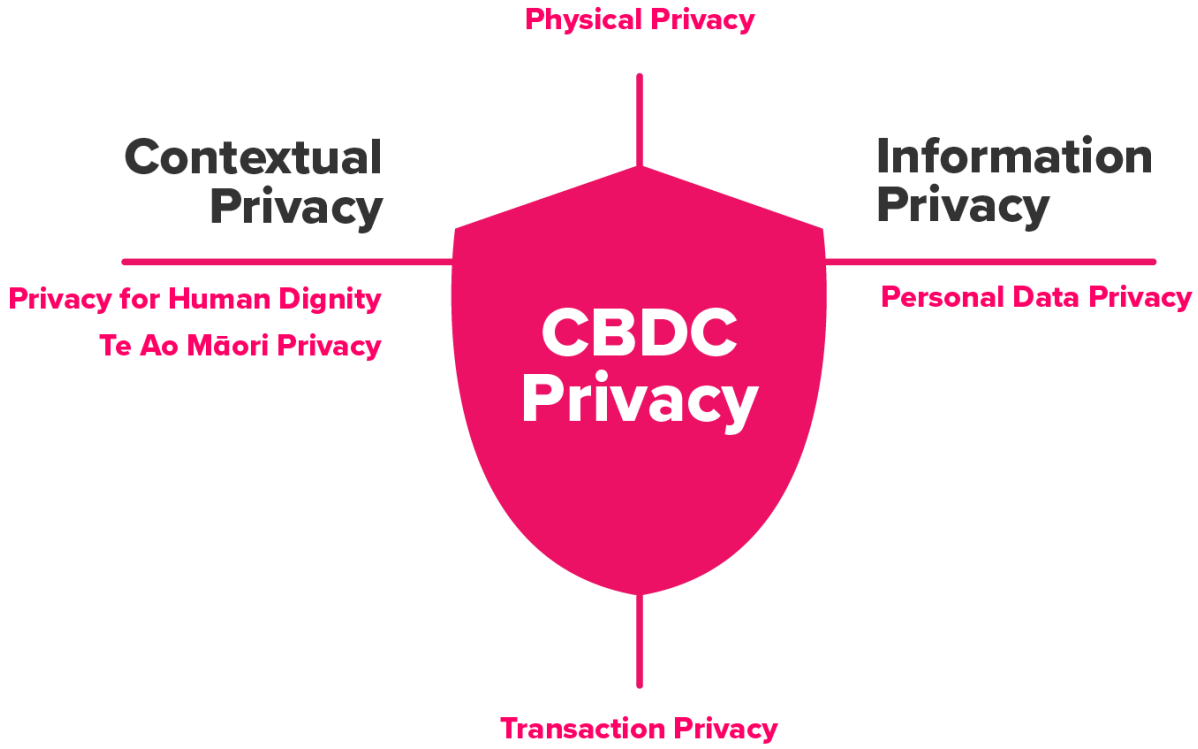
- Forty-five percent of respondents to the Privacy Concerns survey disagreed with the statement "I feel in control of how my personal information is used by businesses" and 35 percent disagreed with the statement "I feel in control of how my personal information is used by government".[16]
- Nine percent of the respondents to the Privacy Concerns survey defined digital privacy as anonymity/no tracking/freedom. [17]
- Some responses to our 2021 Issues Paper expressed concern that their personal information could be used for coercive purposes, even though such use of data would be outside the legal use of data in the Privacy Act 2020. "I would feel much more comfortable with a CBDC if there was legislation in place that ensured the safety, privacy & sovereignty of New Zealand people regarding their money."

3 A New Zealand privacy ontology and legal protection

Information and contextual privacy are not entirely separate concepts. This note uses an ontology to demonstrate the interconnected properties between these concepts (Figure 2). We do not attempt to provide an exhaustive definition of privacy, nor the most precise. Instead, this privacy ontology captures what is relevant for designing a privacy-centric digital cash.

13 See for example Benn (2017 and Bloustein (1964).
14 Westin (1968)
15 A High Court decision in 2021, following two consecutive judicial reviews in November and December, compelled Te Whatu Ora Health New Zealand to release data of unvaccinated Māori in the North Island to the Whanau Ora Commissioning Agency. This decision gave guidance about the discretionary data release in the Privacy Act 2020 and Health Information Privacy Code 2020 where there are compelling circumstances, in this case, the serious threat to public health, Tiriti o Waitangi and tikanga Māori. [2021] NZHC 3319 6 December 2021.
16 OPC (2020a).
17 OPC (2020a).

Figure 2: New Zealand's privacy ontology



Source: Reserve Bank.

The components relevant to information privacy are summarised as:

i. personal information, e.g. name, birth dates and credentials.

ii. physical information, e.g., photographs of individuals, location data.

iii. transaction information, e.g., purchases.

The components that need to be upheld to ensure contextual privacy are summarised as:

iv. A te ao Māori perspective on privacy and Māori data sovereignty, e.g., the ability for Māori to own and use their data for self-determination, and the consideration of collective privacy as well as individual.

v. privacy as human dignity e.g., individuals who experience a loss of information privacy may also experience a loss of human dignity.

vi. physical privacy e.g., the ability to be left alone, including physically, emotionally and in thought.

vii. transaction privacy, e.g. aggregate transaction data can be used to influence communities, regardless of whether individual transactions are private.

The following sections explain each component in more detail and reference their legal provisions.

3.1 Personal information (Information privacy)

Personal information privacy is a popular and well-understood aspect of privacy. Alan Westin in Privacy and Freedom (1968) set out a founding description of privacy in law as control over when, how, and to what extent information about a person is communicated to others.[18] Waldo describes privacy as relating to restrictions on others' access to, and control over, one's personal information.[19] 'Securing and protecting personal information, including financial information' was the most popular definition of digital privacy in an Office of the Privacy Commissioner survey (31 percent of respondents).[20]

The Privacy Act 2020 protects the use of and access to personal information. Personal information is defined as any information about a person that could identify them, this includes basic information like names and contact information and can also include other information such as a pictures, social media opinions, location, medical and educational history.

The Privacy Act 2020 sets out principles to protect personal information, these are summarised by the Privacy Commissioner as:

- you know when and why your information is being collected,
- your information is used and shared appropriately,
- your information is kept safe and secure, and
- you can get access to your information.[21]

As mentioned, under the Privacy Act 2020 individuals are entitled to request correction of their personal information. Agencies who hold that personal information must take reasonable steps to the circumstances to ensure that the information may be lawfully used, is accurate, up to date, complete, and not misleading. Such a correction may be by way of a deletion of information.[22] Deletion of information is most likely when the information is incorrect, or the individual wasn't aware of the data collection.[23]

Box A: The Privacy Act 2020 and Unique Identifiers

Creating a unique identifier for users in lieu of personal information comes with its own privacy requirements under the Act. Relevant to a digital form of cash, the definition of personal information includes unique identifiers, which are subject to further regulation. Unique identifiers are individual numbers and reference numbers employed to identify a user without (or in conjunction with) other personal information.

The Act only allows these identifiers to be created where necessary [Part 3(1), Section 22 Principle 13]. The Privacy Commissioner has powers under the act to monitor the use of unique identifier schemes, per section 17 of the Act. A government agency cannot issue

18 Westin (1968).
19 See Waldo (2007).
20 (2020a).
21 privacy.org.nz/your-rights/your-privacy-rights/.
22 Part 3(1), Section 22 Principle 7.
23 Office of the Privacy Commissioner (2022).

an identifier for use across all government agencies but can share the identifier with others where necessary.

3.2 Transaction privacy (Information and contextual privacy)

Transaction privacy relates to information of sales or purchases and the right to make transactions without interference from the others. It fits within both information and contextual privacy definitions.

Transaction data can be collected by individuals and businesses to provide a history of a person's transactions or build aggregated customer shopping trends. Viewing transaction data can breach personal information privacy. Aggregation can be used to remove identifiable personal information, but in many cases the de-identified data can be re-identified by a motivated researcher. This is because data about a person can reveal personal information. For example, web search browser histories. It can also be combined with another dataset to identify the person.

Even if individuals are not re-identified, aggregated data can be used to influence personal decisions. This is because firms can use marketing tactics or price discrimination on groups of people, based on insights derived from aggregated transaction data.[24] For example, cosmetics company 100% Pure collects aggregated data on what website visitors are most likely to leave the site without a purchase, it then offers those visitors a greater discount than others.[25] Individuals are therefore personally impacted by inferences made from aggregated data, either they are offered a larger or smaller discount depending on their browsing characteristics. Digital Identity New Zealand also describes how transaction histories, linked to personal information, allows purchases to be influenced by aggregated demographic and financial information. Influencing people's shopping options based on aggregate data may cause them to feel that they are not fully free to make their own choices.

In addition, sharing or using transaction data can have competition implications. A large firm with greater market power may be able to capture more information and thus more effectively price discriminate than smaller peers. This may be resolved by greater information sharing among firms, although this is at odd with privacy. One solution proposed by Garratt and van Oord (2019) is a privacy preserving payment mechanism akin to cash, that reduces the opportunities for individuals to give away their personal information when making transactions.

Transaction data and its potential impact on personal freedom and autonomy captures concerns raised by some respondents to the 2021 Issues Paper. These concerns included whether the government would have access to data about an individual's transactions (either individually or aggregate) and use that information to influence (or limit) future transactions.

24 (2019).
25 IRIS Pricing Solutions (2022).

Figure 3: New Zealand transaction privacy concerns from the Digital Identity New Zealand survey

Source: Digital Identity New Zealand Survey, 2019.

Box B: Privacy as a Public Good

Garratt and van Oord (2019) provide an argument for considering privacy as a collective or public good that requires consumers to protect it. They suggest that one individual forgoing privacy in a transaction can be used to identify other consumers with similar spending patterns even if the other consumers have made efforts protected their personal information. Information extracted from payments data is used to cluster potential customers into groups, who may then be offered the same products with different prices.

They note important effects of lack of privacy, as evidenced by commercial payments platforms:

1. "Commercial payments platforms can monetize user data". They may combine transaction data with other data for marketing or risk analysis. This data may also be shared with third parties.

2. Governments can also use transaction data to generate credit scores and determine discounts, waivers, punishments, and penalties.

Aggregated transaction data can be used to price discriminate for large groups of similar customers. These groups are identified by the information willingly given by a few individuals. This price discrimination reduces the purchasing power of individuals who earn more money.

Privacy is a public good as individuals may not be incentivised sufficiently to protect their individual information because the cost is spread among society, rather than being born by the individual who shares their information.

Reference: Garratt R and M van Oordt (2019) 'Privacy as a public good: a case for electronic cash', Bank of Canada *Staff Working Paper*, 2019 – 24.

3.3 Physical privacy (Information and contextual privacy)

Physical privacy relates to our physical person, property, and images. It was one of the first definitions of privacy endorsed in the modern common law system. In 1890, Warren and Brandeis defined privacy as 'the right to be let alone'. This protects against intrusions from others and the right to protect your information, body, and physical property.[26]

Physical privacy is a component of both information and contextual privacy. It includes information about our physical image such as photos. It also refers to the freedom to be left alone. Going back to Alan Westin's functions of privacy, physical privacy allows people a release from role-playing and a time for self-evaluation.[27] These additional attributes of physical privacy, which are also referenced in the Warren and Brandeis definition,[28] make it a component of contextual privacy.

In one sense, the increased use of online interactions may have lessened the focus on physical privacy as people can preserve their physical privacy in terms of photographs or nearness to others. However, physical privacy is still relevant, particularly for transactions. For example, people can provide their photograph to open a mobile wallet or use their biometrics to instruct a payment. Security cameras can also capture identifying information about an individual even if they are making a cash payment in store.

There are a range of New Zealand laws that protect aspects of physical privacy. These are summarised by Kim (2019) as "Broadcasting Act 1989; Crimes Act 1961, ss 216H (criminalises intimate visual recordings of another person); … Harassment Act 1997 (bodily privacy); … ; Residential Tenancies Act 1986, s 38 (spatial privacy); and Search and Surveillance Act 2012."

3.4 Privacy as an aspect of human dignity (Contextual privacy)

Human dignity is the belief that all people hold special value and is at the heart of human rights. Benn and Bloustein in the 1960s and 1970s were first to describe privacy as human dignity, seeing it as a fundamental right.

Westin (2003) says it is environmental factors, class, and race that "shape the real opportunities people have to claim freedom from the observation of others".[29] He outlined several stages of privacy concern (in the United States primarily) and connected them to specific relationships which required different approaches to privacy. Significantly, he listed the first relationship to challenge

26 This definition of privacy was argued to be distinction from personal property protection and goes further than protecting information. It also protected personal "productions" i.e. writings and emotions. Warren and Brandeis (1890).
27 (1968).
28 (1890).
29 (2003).

privacy was the relationship between citizen and government and the last as consumer and business.[30]

Privacy as an aspect of human dignity may be behind many of the concerns submitted to the Reserve Bank in response to our 2021 Issues Papers.[31] Many submitters felt that a digital form of money issued by the Reserve Bank could affect their human dignity, and potentially be used to control people. Many of the individuals used the framing of 'human rights' to assert their control and freedom over their own data.

- "With the government control over our lives increasing, you haven't properly explored the added control this gives the government over its citizens. In this current climate these are very concerning probabilities. Governments do not easily give back powers once they have these levels of control and it looks like this is adding to that" – Cash system redesign Issues Paper submission
- "The government have way too much control over private citizens money and lives." – 2021 Issues Paper submission

There are also specific groups affected by government data collection in socio-cultural ways. For example, one LGBTQ (lesbian, gay, bisexual, transgender, queer or questioning, or another diverse gender identity) group indicated potential privacy issues relating to previous names or legal names when using their bank accounts and other forms of identification. Therefore, there are both individual and group concerns about the way privacy might impact their dignity and sense of freedom or control.

Privacy as human dignity has relevance to several international and national human rights laws. Article 12 of the Universal Declaration on Human Rights and Article 17 of the ICCPR affirm a fundamental right to privacy. The latter instrument has been agreed to by New Zealand to be a legally binding document. Article 17 says:

i. 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.

vi. Everyone has the right to the protection of the law against such interference or attacks.

The Bill of Rights Act 1990 does not give New Zealanders an explicit right to privacy. However, New Zealander's rights to privacy have been upheld in common law, notably in Hosking v Runting.[32]

3.5 Te ao Māori approach to Privacy

New Zealand must also consider a te ao Māori approach to privacy. This is distinct from Western European approaches embedded in the New Zealand legal system. Māori legal academics have discussed distinct Māori privacy needs, which reflect Māori worldview, as well as experiences with colonisation and government.[33]

30 Ibid.
31 Reserve Bank of New Zealand (2021a) and Reserve Bank of New Zealand (2021b).
32 Hosking v Runting [2004] NZCA 34 (25 March 2004); [2005] 1 NZLR 1; (2004) 7 HRNZ 301.
33 New Zealand is also a signatory to the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) for the collection, ownership and application of data pertaining to indigenous peoples.

Tikanga Māori considers the concepts of privacy and the interrelated nature of individual privacy needs with those of others in a person's hapū (family) or iwi (tribe). That is, privacy is considered at both a personal level and a collective level.

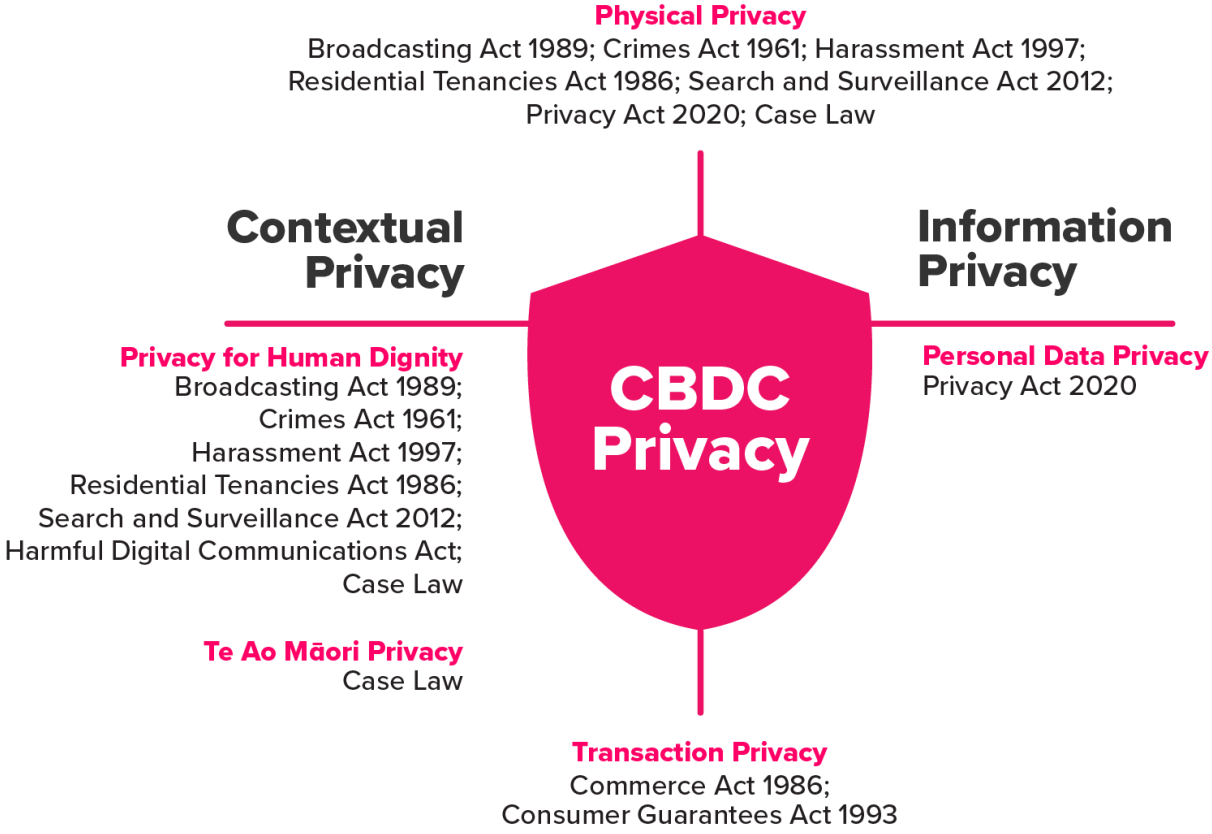
Māori data sovereignty and Māori data governance (MDGov) reflect a te ao Māori approach to privacy. Māori data sovereignty refers to the rights Māori have to data that relates to Māori, and how it is defined, collected, accessed, interpreted, and used. Māori data is defined by Te Mana Raraunga, the Māori Data Sovereignty Network, as 'digital or digitisable information or knowledge that is about or from Māori people, our language, culture, resources, or environments'.[34]

A MDGov model was developed by the Data Iwi Leaders Group and Statistics NZ and captures their vision for self-determination, values around data, and pillars (pou) to ensure Māori authority over Māori data.[35] The vision for the model is that iwi, hapū and Māori organisation business and communities can pursue their own goals for cultural, social, economic, and environment wellbeing and to address inequalities.

The MDGov model treats Māori data as tapu, meaning restricted or sacred, or tāonga. The model notes that "A major challenge for Māori privacy protection is that the Privacy Act 2020 does not include specific Tiriti, tikanga or Māori privacy considerations. The only direct mechanism for consideration is through section 21(c) of the Privacy Act 2020, which requires the Privacy Commissioner to take cultural perspectives on privacy into account." However, te ao Māori privacy has been upheld in common law, notably in a precedent setting case Te Pou Matakana Limited v Attorney-General.[36]

34 Royal Society Te Apārangi (2023).
35 Kukutai et al (2023).
36 Ibid.

Figure 4: Privacy ontology with legal provisions



Source: Reserve Bank.

4 Designing privacy-centric digital cash

To achieve broader trust and buy in to digital cash it is important that its design addresses the privacy needs of the New Zealand community. Given our ontology, we can conclude that to ensure privacy needs are met, digital cash must protect informational privacy, as well as personal freedom and autonomy in how we live and spend our money. It must also uphold te ao Māori privacy.

4.1 Information privacy design recommendations

When designing digital cash for New Zealanders information privacy must be understood and addressed. To the extent that data is collected, the Reserve Bank should apply the principles on collection, retention and use of information set out in the Privacy Act 2020.

In particular, the Reserve Bank must also consider who holds the data of end users. The data on end users could be held by the Reserve Bank, a digital cash ecosystem service provider, or an independent entity.[37] The Reserve Bank does not have commercial interests in consumer data, but service providers in the digital cash ecosystem may. Establishing information governance policies and monitoring third party adherence to these policies would likely be required.

The design of the digital cash product can also be used to govern information management. A digital cash design that collects as little customer data, particularly sensitive or identifying data, as

37 BIS (2021).

possible will give greater information privacy protection. To this end, the design of digital cash must also establish early on how transactions will be authorised, whether the user will be identified and what role the Reserve Bank will play in collecting and accessing personal data.

Digital cash design must also consider how any Māori data collected would be consented, identified, classified, stored, and made available to iwi and hapū for their use as per the MDGov model.

Perceptions of informational privacy are affected by the cybersecurity of the product or institution that collects data. Therefore, digital cash design must also address concerns about cybersecurity.

4.2 Contextual privacy design recommendations

A key conclusion of this note is that adhering to the Privacy Act 2020 will not be sufficient to meet user privacy expectations. Providing for informational privacy will also not be sufficient. The design and governance of digital cash must also provide for a contextual view of privacy.

Specifically, digital cash design should consider how to embed personal autonomy and freedoms into the use of the digital cash. Some recommendations are made in Table 1.

In addition, the Reserve Bank should assure people of the privacy protections that it designs into digital cash. The Reserve Bank and third parties should also communicate well with end users, so they understand what information is being collected and how it is being governed and used. The Reserve Bank should also explore the role of third parties and technical solutions in digital cash and its ecosystem.

The privacy considerations for a digital form of cash are summarised in Table 1.

Table 1: Privacy design implications for digital cash

Privacy dimension	Implications for digital cash design
Personal information	Must comply with legislation and have good data governance, while collecting minimum personal data for AML/CFT compliance. Communicate to, and educate, users on the way their data will be accessed, collected, used, and stored. Give users control over their data including what is shared and when, and the ability to delete or retract their information from the digital cash ecosystem.
Physical information and privacy Contextual privacy implicates physical privacy when users fear coercive responses to data collection.	Consider the role of physical information in the digital cash ecosystem and ensure that physical information is protected. Address user fear when collecting data.

Privacy dimension	Implications for digital cash design
Transaction information and privacy Some users have privacy concerns about their transaction histories, and freedom to make future transactions.	Appropriately govern who has access to transaction data and how that data can be used and shared.
Te Ao Māori perspectives Te Ao Māori conceptions of privacy are distinct from western concepts and reflect a collective approach to knowledge.	Identify what Māori data might be collected in the digital cash ecosystem and consider how to implement the Māori data governance model for that data support Māori data sovereignty.
Privacy as human dignity Privacy affords personal autonomy and freedom.	The digital cash ecosystem should ensure people's right to live freely without interference or control of another (government or business). People should feel empowered that they can make their own choices and live and spend as they want to when using digital cash. People should not be required to give up autonomy to use the digital cash.

Source: Authors' elaboration.

5 Constraints on a privacy-centric digital cash

A digital form of cash, just like other digital forms of money, requires sharing data to verify transactions. This imposes minimum requirements on what data must be collected and who it is shared with in a digital cash system. These requirements, as well as a public desire to reduce crime, and commercial incentives to build data driven products create tension with a fully privacy-centric digital cash. These are explained below.

Security: A fundamental constraint of privacy in digital cash is the need to address the double-spend problem with digital money forms. Digital money is represented by a string of bits and like any electronic information can be copied and pasted. This means that there is a need to ensure that digital money cannot be spent more than once - this is called the 'double-spend problem'.[38]

Existing payments systems and commercial bank accounts use a trusted central agent to manage this risk. To spend money in a transaction account, some kind of digital 'authentication' needs to take place. This involves messaging to check that funds exist in the payer's account and that these funds can be spent. Cryptoassets and distributed ledgers, also employ a way to prove the authenticity of a payment. They build consensus among the community to verify that the payment is valid and should be added to the ledger. This can be done with digital signatures that rely on cryptography and proof of knowledge and a consensus mechanism.

The base requirement to verify the authenticity and ownership of digital money means that some form of data is collected and shared. This is unlike cash, where the authenticity of the payment

38 Wadsworth (2018).

depends on verifying a physical banknote or coin in-person. In addition, digital money by its nature generates data. Table 3 compares the privacy features of different money forms.

Table 3: Privacy features of digital cash, physical cash, bank transaction accounts and cryptoassets

	Digital cash	Physical cash	Transaction accounts	Cryptoassets on a distributed ledger
Proof of ownership	Holder, personal ID, or proof of knowledge (TBD)	Holder	Personal ID	Proof of knowledge
Transaction record	Electronic data	Individual memory or manual data entry	Electronic data	Electronic data
Data governance	Managed by central bank or outsourced	None	Managed by commercial banks	Either none or managed by one or several parties depending on the DLT arrangement

Source: adapted from Reserve Bank (2021a).

Reduce crime: Anonymous transactions can support tax avoidance and tax evasion, as well as other types of criminal activity.[39] Governments while seeking to uphold citizens personal autonomy, also place boundaries on criminal behaviours. The privacy-centric design of digital cash must address this tension. In particular, digital cash may need to comply with the anti-money laundering and countering financing of terrorism (AML/CFT) Act 2009. In New Zealand, there is no simple dollar boundary for compliance with the AML/CFT Act 2009. AML/CFT reporting thresholds are different across payment types and any payment is subject to 'suspicious activity reporting'.

Innovation: Customer data may be used by third parties to develop better money services. People may opt to forgo their personal and transaction privacy to benefit from greater convenience. The tension with this is trust, if the data required compromises privacy by too much then users may opt out of using digital cash. A second tension is that some people may be prepared to give over their transaction data, which may erode the transactional privacy of others who have not given their information. The design and governance of a digital cash must carefully balance these competing interests.

Transaction speed: There may be constraints on highly private digital cash designs depending on the way privacy is designed into the system. For example, too much encryption may reduce the speed and volume of transactions.[40]

6 Conclusion

The Reserve Bank is researching how to embed privacy in a potential future digital form of cash. Privacy is clearly important to New Zealanders and plays an important role in user uptake. The

39 Reserve Bank (2021).
40 Darbha and Arora (2020); World Economic Forum (2021).

privacy ontology in this paper recognises that privacy is a multi-faceted concept. It shows that the design of digital cash must take account of contextual privacy needs in addition to information privacy needs.

The privacy considerations for digital cash have been embedded into the digital cash privacy principle in Table 2. The full list of digital cash principles are set out in the Digital Cash in New Zealand Consultation Paper.

Table 2: Digital cash privacy principle

Principle	Supporting criteria
Private Your information and lives will be kept private, and not influenced by the Reserve Bank when using digital cash. To achieve this, we must build in **information governance** and **assurance**.	**Information governance** Your privacy will be protected by the Privacy Act 2020 and good data governance principles. The Reserve Bank will collect as little data as possible and won't be able to see your personal information or how you spent your money. You will have a choice on how your information is used, stored, shared, and deleted. Digital cash will uphold Māori data sovereignty. **Assurance** You can feel confident in your freedom and rights when using digital cash.

References

Digital cash consultation publications

To support the Digital Cash consultation the following notes and reports are available here.

- Reserve Bank (2024a) 'Digital cash in New Zealand' Consultation Paper.
- Reserve Bank (2024b) 'Designing a digital cash ecosystem', *Digital Cash Consultation Note*, No 1.
- Reserve Bank (2024c) 'Innovation and reliability opportunities for digital cash', *Digital Cash Consultation Note*, No 2.
- Reserve Bank (2024d)' Inclusion opportunities for digital cash', *Digital Cash Consultation Note*, No 3.
- Accenture and the Reserve Bank of New Zealand (2024) 'Central Bank Digital Currency', Strategic Insights Dossier, April.
- GravitasOPG and One Picture (2023) 'User needs for money management and payments', Qualitative research report, April.
- The digital cash storyboard presented to the Reserve Bank of New Zealand Board, February 2024.

References

Bank for International Settlements, (2021) 'Central bank digital currencies: system design and interoperability', BIS Report No. 2.

Barry B, (2001) 'Studying the Internet Experience', report for Publishing Systems and Solutions Laboratory, HP Laboratories Bristol, 26 March 2001.

Barth S, and M de Jong (2017) 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review', *Telematics and Informatics* Volume 34, Issue 7, pp 1038-1058.

Benn S, (2017) 'Privacy, freedom, and respect for persons', In privacy and personality, pp 1-26, Routledge.

Bloustein E, (1964) 'Privacy as an aspect of human dignity: An answer to Dean Prosser,' NYUL rev 39, pp 962.

BNZ (2021) 'BNZ Digital Skills for Life in Aotearoa'.

Darbha S, and R Arora (2020) 'Privacy in CBDC Technology', Bank of Canada *Staff Analytical Note* 2020-09.

Digital Identity New Zealand (2019) 'Providing a Benchmark Understanding of Digital Identity Among New Zealanders'.

European Central Bank (2019) 'Exploring anonymity in central bank digital currencies' *In Focus*, Issue no 4, December.

Financial Markets Authority (2022) 'Consumer Experience of the Financial Sector', Survey July 2022.

Garratt R, and M van Oordt (2019) 'Privacy as a Public Good: A Case for Electronic Cash', Bank of Canada Staff Working Paper, No 2019-24.

IRIS Pricing Solutions (2022) 'How Does Data Analytics Impact Pricing Strategy?', Blog post, https://www.pricingsolutions.com/pricing-blog/data-analytics-impact-pricing-strategy/ accessed September 2022.

Kim, J (2019) 'The Case for Reform: A Right to (Access-Based) Privacy in the New Zealand Bill of Rights Act 1990', *Public Interest Law Journal of New Zealand*, 6, pp 137.

Kukutai T, K Campbell-Kamariera, A Mead, K Mikaere, C Moses, J Whitehead and D Cormack (2023) 'Māori data governance model', Te Kāhui Raraunga.

Liddicoat J, (2017) 'Including privacy in a modern constitution', Office of the Privacy Commissioner, https://www.privacy.org.nz/blog/including-privacy-in-a-modern-constitution/ accessed 12 February 2024.

Mulligan, D, C Koopman and N Doty (2016) 'Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy', Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Vol 374, No 2083, pp 20160118.

New Zealand Parliament (2020) 'Privacy Act 2020', Legislation, Part 3(1), Section 22, Principle 13.

NZCVS Cycle 5 (November 2021 – November 2022).

Office of the Privacy Commissioner (2020a) 'Privacy survey 2020'.

Office of the Privacy Commissioner (2020b) 'Privacy Act 2020 and the Privacy Principles', https://www.privacy.org.nz/privacy-act-2020/privacy-principles/ accessed 4 March 2024.

Office of the Privacy Commissioner (2020c) 'Privacy concerns and sharing data', presentation of UMR Research Survey, April 2020.

Office of the Privacy Commissioner (2022) 'Can I remove my personal information?' https://privacy.org.nz/tools/knowledge-base/view/112#:~:text=Under%20the%20Privacy%20Act%2C%20if,removal%20from%20the%20agency's%20records, accessed September 2022.

Ohm P, (2009) 'Broken promises of privacy: Responding to the surprising failure of anonymization', UCLA l. Rev., 57, 1701.

Reserve Bank of New Zealand (2021a) 'Future of Money – central bank digital currency', *Issues paper*, September 2021.

Reserve Bank of New Zealand (2021b) 'Future of Money - Cash system redesign', *Issues paper*, November 2021.

Royal Society Te Apārangi (2023) 'Mana Raraunga Data Sovereignty'.

Statistics New Zealand (2018) 'Is data taonga?' A panel discussion hosted by Data New Zealand, 13 Nov 2018, https://www.data.govt.nz/blog/new-videos-explore-are-data-taonga/#data-taonga-english, accessed 4 March 2024.

United Nations (1966) 'International Covenant on Civil and Political Rights' adopted 16 December 1966, Article 17.

Wacks R, (1980) 'The Poverty of Privacy', *Law Quarterly Review* Vol 96, Issue 1 (January 1980), pp 73-89.

Wadsworth A, (2018) 'Decrypting the role of distributed ledger technology in payments processes', Reserve Bank New Zealand *Bulletin* Vol 81, No 5.

Waldo J, H Lin and L Millett (2007) 'Engaging Privacy and Information Technology in a Digital Age', Committee on Privacy in the Information Age, National Research Council Published by the National Academies Press, Washington, D.C., 2007.

Warren S, and L Brandeis (1890) 'The right to privacy', *Harvard Law Review*, Vol 4, No 5, pp 193 - 220, 15 December.

Westin A, (1968) 'Privacy and freedom', *Washington and Lee Law Review*, Vol 25, No 1, p 166.

Westin A, (2003) 'Social and Political Dimensions of Privacy', *Journal of Social Issues*, Vol 59, No 2, 2003, pp 431—453.

World Economic Forum (2021) 'Privacy and Confidentiality Options for Central Bank Digital Currency', White Paper published for Digital Currency Governance Consortium White Paper Series (6/8) November 2021.