Privacy Principles for a Digital Dollar

Authored by The Digital Dollar Project with expert insight from our Privacy Sub-Committee

Document Purpose:

This document is intended to express first principles that the Digital Dollar Project believes are important to the success and adoption of a U.S. Central Bank Digital Currency (CBDC). The privacy protections of the U.S. Constitution[1] and our democracy's commitment to individual privacy offer a unique opportunity for U.S. digital money to be more appealing to users then other, less-private digital currencies, solidifying its position as the world reserve currency. The principles expressed below are meant to inspire robust debate about their application in terms of both the technology selected to undergird a U.S. CBDC and the public policies that support optimal balances of privacy and related values against security, monetary management, and other priorities.

Introduction:

As central banks begin exploring, testing, and implementing CBDCs, it is important to recognize how the monetary landscape has changed. For more than a century, the central banks of many countries have had exclusive or near-exclusive control over the structure, production, and management of the currencies used within their territories. The stability, trustworthiness, and general acceptance of modern currencies have been important pillars for growth of financial and consumer markets and for global economic growth. Ubiquitous fiat currencies issued by stable governments have largely met the needs of users by acting as medium of exchange, stores of value, and units of account. Countries where monetary stability lacks, of course, have seen financial dislocation, market instability, economic loss, and sometimes political disorder.

In recent decades, trade and financial flows have globalized and become increasingly connected by the internet and modern technologies. New forms of currency have emerged that are available 24/7/365, globally accessible, and digitally native. Systems such as bitcoin, aiming to be "trustless" and censorship-resistant, have made headway at least as mediums of exchange, and countless other "cryptocurrencies" are on offer. Central bankers and other policy makers must recognize that these are increasingly being used as substitutes for government fiat currencies. A cryptocurrency that knits together the right properties could become the functional currency for any given country, trade sector, geographic region, or other political, social, or commercial environment.

If CBDCs are ill-designed for consumer and institutional preferences, they risk ceding ground in this newly competitive field. One of the demands users of money have is privacy. The European Central Bank recently published the results of their three-month long comment period on the potential of a EURO CBDC. After distilling over 8,000 comments, the number one most requested feature, representing 41% of all replies was privacy of payments.

The Digital Dollar Project believes that, if there is to be a U.S. CBDC, it must retain and increase the dollar's global strength by adopting American ideals of individual privacy and by adapting financial privacy policies to the new digital environment. Consumers benefit profoundly from having privacy, just as businesses, investors, fiduciaries, and governmental units benefit in myriad ways from confidentiality. Retaining those benefits, while striking appropriate balances between privacy/confidentiality and other social goods, can be a key differentiator of a U.S. CBDC.

Principles:

Privacy is "of the essence" for living in a free country that respects individuals and individual rights. In the American tradition, people may pursue privacy—keeping personal information to themselves—for any reason or

[1] A right to information privacy is not specifically established by the Fourth Amendment, [2] but for the last half-century courts have protected privacy using a doctrine called the "reasonable expectation of privacy" test. [3]

no reason. This type of authority over oneself, one's information, and one's relationships strengthens and empowers people in many ways, including by preserving their political and legal independence. Privacy protects the freedom to support controversial causes. Privacy protects victims of stalking, harassment, fraud, and theft. Privacy gives people autonomy and choice as to how they engage with society.

The protections for personal information that foster privacy do parallel good when used by organizations to protect the confidentiality of their information. Businesses large and small must protect confidential business relationships and plans. Confidential financial flows safeguard and secure relationships between attorneys and clients, between doctors and patients, and among political interest groups. Confidentiality protects investors in executing their strategies and in keeping their assets safe. Government entities of all kinds must enjoy and use privacy and confidentiality protections, too. Aid programs must be able to accord privacy to beneficiaries, for example. The military must be able to protect against revealing strategy, planning, and activity through financial flows.

The literal protection of information is one thing. "Privacy" is also a word at the center of a suite of related values, including security, inclusion, fairness, and transparency. The system on which a U.S. CBDC runs should be highly secure itself, of course. The interfaces by which people access U.S. CBDC should make them no more susceptible to theft and fraud than they are in today's financial systems. By lowering costs, the U.S. CBDC should make financial services more available to more people, reducing the rolls of the un- and underbanked. The U.S. CBDC should operate transparently, so that users both individual and institutional do not have to rely on promises about how the system functions technically. They should be able to confirm for themselves that protections for these values are built into the systems.

Though the benefits of privacy and confidentiality are substantial, when appropriate legal standards are met, our laws enable law enforcement and national security to access certain types of otherwise private information. The other values related to privacy also live in a world of trade-offs. After reciting the principles immediately below, the next section begins to explore questions that arise in their application, particularly emphasizing how the new digital environment may call for reassessment of current policies affecting the trade-off between privacy and law enforcement/national security interests.

The Digital Dollar Project believes a U.S. CBDC should be:

Private - People should be able to use a U.S. CBDC without making themselves subject to undue corporate tracking or government surveillance. People may benefit from above-board, contractual sharing of information with financial services providers, or they may refuse it. Law enforcement access to CBDC usage data should be strictly controlled by due process, and other applicable U.S. law, including the Fourth Amendment.

Secure - A U.S. CBDC should improve and not degrade people's security against theft, hacking, illegal seizure, and fraud. It should provide people with more secure ways to handle money individually, on a system that is secure against attacks and legally protected, with money handling tools that protect against the frauds that an unfamiliar technology might otherwise allow.

Accessible - A U.S. CBDC should improve Americans' and global dollar users' access to financial services. Because it is a more efficient system, it should cost less to engage in basic financial transactions. And as an open system, it should draw competition into financial services that produces better services at lower costs.

Transparent - The system on which a U.S. CBDC runs should be operationally transparent so that a variety of parties – governments, NGOs, businesses, and academics – can independently assure themselves about its technical functioning, its security, and its resistance to impermissible monitoring or other exploitation.

Applying Privacy Principles to a U.S. CBDC:

The application of privacy principles to a U.S. CBDC should be driven by an important premise: Digital currencies will be fundamentally different from what currently exists. Thus, the policies that balance privacy against other interests may require fundamental reconsideration.

To illustrate the depth of change that may be called for, consider that the existing anti-money laundering framework in the United States originated in the 1970s, with many of the important Supreme Court cases in this area decided at the same time. These laws were stood up and considered in the courts at a time when rotary phones were new technology.

An anecdote can put in perspective what it means to operate with so different a technology:

> Prior to the rotary phone, callers relied on operators to move calls manually through the system. The rotary phone sought to automate this process, making it possible for individuals to make phone calls without an operator as middleman. In the United States, the North American Numbering Plan allowed direct dialing by assigning numerical area codes to different cities.
>
> The allocation of numbers was driven not by the organizational logic of the country, its geography, but by the physical design of the phone. Prominent and densely populated cities were assigned area codes that required the least time to dial. Low numbers required turning the rotary dial only a short distance before releasing it to signal the number. That is why New York City was assigned 212, Los Angeles 213, and Detroit, 313; it took the least time and effort to dial these numbers. At base, area codes were allocated by the intersection of population and how long it took for an individual to physically dial a number.

A different age and new technology will require different calculations and potentially a novel approach. This will likely be especially true in the area of financial privacy. The U.S. Supreme Court has begun to grapple with the consequences of the new technological environment.

Privacy in the U.S. Supreme Court

Fourth Amendment privacy protections in the digital era are evolving, a process that may revise the balance between privacy with other societal priorities. A right to information privacy is not specifically established by the Fourth Amendment,[2] but for the last half-century courts have protected privacy using a doctrine called the "reasonable expectation of privacy" test.[3]

In the last two decades, greater use of digital technology has re-opened the question of how the Fourth Amendment's protections apply, with an often-expressed goal of preserving "that degree of privacy against government that existed when the Fourth Amendment was adopted."[4] When government agents have used novel

[2] The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[3] The test is, roughly: If government agents have upset a person's reasonable expectation of privacy in their person, house, papers, or effects, then a search has occurred, and it must meet Fourth Amendment standards. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[4] *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *United States v. Jones*, 565 U.S. 400, 406 (2011); *Id*. at 420 (Alito J., concurring in the judgment).

sense-enhancing technology on a home, for example, the Court has treated that as a search without respect to expectations.[5]

The question for a U.S. CBDC will be what rules apply to gathering and examination of data produced by its operation and use – whether and when gathering is a seizure, and what examinations of data are a search. A sub-doctrine of "reasonable expectations" called the "third-party doctrine" would seem to apply. With roots in government access to financial transaction information,[6] the third-party doctrine holds that information shared with a third-party is not subject to constitutional protection and is therefore subject to seizure and search according to lower statutory standards.

Supreme Court opinions have openly questioned the third-party doctrine, though.[7] In 2018, the Court declined to extend the doctrine to data produced by cell phones that can track an individual's movements.[8] And it has recognized that data held by cell phones represent constitutionally protected "privacies of life."[9]

It is of utmost importance to see that the protections of the Fourth Amendment apply to data produced by a U.S. CBDC that reflects individualized transactions, personal and business relationships, political leanings, religious practice, and more. The Supreme Court appears to be moving in that direction. Other areas of law should be revised and modernized, too.

Privacy and Financial Crime

Fighting financial crime is extraordinarily important, but it is important to do so while preserving privacy. It is equally important to increase the number of people who have access to financial services. The balance between privacy and security may not be struck correctly by current policy. In tandem with the creation of a U.S. CBDC, those policies should be reopened for discussion.

The data flows produced by a U.S. CBDC could give the government unprecedented surveillance capabilities and power to control monetary flows. The government could have enormous ability to detect and disrupt financial crime because it would have a level of transparency nonexistent under our current cash-based and distributed system.

However, this may come at too much cost to privacy and related societal priorities. The current system does not naturally report all financial transactions and transaction flows to the government. Instead, policies require reporting of select information, a natural limit on government access. For example:

- Banks only report certain types of information to the government, such as when they detect suspicious activity or through currency transaction reports. They do not report every single transaction;
- Prosecutors can only get information via subpoenas when they have suspicion that the law is being violated;
- Search warrants are only granted after review by a judge and a probable cause finding.

---

[5] *Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search-at least where (as here) the technology in question is not in general public use.").

[6] *See United States v. Miller*, 425 U.S. 435 (1976).

[7] *Jones*, 565 U.S. 400 at 417 (Sotomayor, J., concurring in the judgment) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.")

[8] *See Carpenter v. United States*, 138 S.Ct. 2206 (2018); *see also United States v. Jones*, 565 U.S. 400, 411 (2012).

[9] *See, e.g.*, *Riley v. California*, 575 U.S. 373, 403 (2014)(quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

There are a number of safeguards built in to our current systems that, on the one hand, enable the disruption of financial crimes, but on the other hand, limit the ability of the government to get access to perfectly licit transactions.

Comparing the present system to the potential of a U.S. CBDC raises a host of questions. What happens when a CBDC potentially gives the government instant access to more information, allows the government to track every transaction, and to program its functioning in numerous ways? How will the Central Bank make decisions about who to restrict access of a digital currency to? Will it do so in the same way that many banks do today where, upon detection of some suspicious or illicit activity, they can cancel the customer's accounts? Will a central bank, upon information suggesting suspicious activity, do the same? What are the methods of recourse should CBDC systems make an incorrect assessment and take erroneous automated action? Will the Central Bank be able to take automated action on individuals, accounts, institutions, or governments? If policies are adversarial to currently marginalized or un- and under-banked populations, the risk of a CBDC further alienating these populations is real and must be considered.

The creation of a U.S. CBDC requires consideration of a new set of rules, regulations, and technologies that do a far better job of detecting illicit activity but also limit the government's ability to access the data of perfectly innocent people. People should be able to use a CBDC, whatever form it takes, with at least the privacy protections they enjoy today.

Conclusion:

The mission of the Digital Dollar is to "advance exploration of a United States Central Bank Digital Currency." In the matter of privacy, the Digital Dollar Project suggests that the foundational principles for a U.S. CBDC should be: assurance of individual financial privacy, enhanced security, greater financial inclusion, and transparency that enhances public confidence. The Digital Dollar Project invites feedback, discussion, and debate on these foundational privacy principles. This new financial technology requires a deep dive into what privacy rights should be in place. A U.S. CBDC will likely require an enhanced CBDC-native framework, based on fundamental democratic norms.