epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Office of Science and Technology Policy

on

Request for Information: Digital Assets Research and Development

88 Fed. Reg. 5,043

March 6, 2023

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the White House Office of Science and Technology Policy's (OSTP) request for information on digital assets and a central bank digital currency.[1] In our view, the creation of an intermediated central bank digital currency (CBDC) could improve financial privacy for individuals if the system is designed to facilitate anonymous transactions equivalent to cash and minimize the amount of data generated about individuals' purchases. We also strongly encourage research into fully anonymous digital cash and fully anonymous credentials.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus on public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has long advocated for robust safeguards to protect consumers from exploitative data collection, usage, distribution, and retention practices.[2] EPIC has played a leading

[1] 88 Fed. Reg. 5,043.
[2] EPIC Comments on CFPB Inquiry Into Big Tech Payment Platforms, CFPB-2021-0017 (Dec. 2021), https://epic.org/documents/epic-comments-on-cfpb-inquiry-into-big-tech-payment-platforms/; Consumer

role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[3] Recently, EPIC provided detailed comments on the impact of artificial intelligence on financial privacy[4] and comments on the potential for a central bank digital currency.[5]

EPIC urges OSTP to prioritize privacy-enhancing technologies when expanding research on digital assets. EPIC particularly urges OSTP to prioritize the most privacy protective forms of digital currencies, not just those that are most obviously designed to prevent money laundering. A privacy-protective CBDC would require close regulation and testing of the underlying protocols, systems, and devices and should be designed as a cash-like digital currency using a token-based system without a persistent digital ledger. Research should equally investigate the possibility of anonymous digital cash and fully anonymous credentials as key components of any future digital payments system.

I. The current digital payments space is under-regulated and rife with surveillance.

In response to Question 1: Goals, sectors, or applications that could be improved with digital assets and related technologies:

The current system for both physical point of sale and online payments is under-regulated and subjects individuals to voluminous financial surveillance. Credit cards, online transactions, and point-of-sale systems all have access to detailed records of individuals' financial transactions, and many of the entities operating these systems are either selling this personal data to brokers, or they

---

Reports and EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), available at: https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; *see generally*, EPIC, Data Brokers, https://epic.org/issues/consumer-privacy/data-brokers/.

[3] *See* EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities* (June 2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.

[4] EPIC Comments on Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, Comptroller of the Currency et al. (Jul. 1, 2021), https://archive.epic.org/EPIC-Financial-Agencies-AI-July2021.pdf.

[5] EPIC Comments to Federal Reserve on Money and Payments in the Digital Age (May 20, 2022), https://epic.org/documents/epic-comments-on-the-federal-reserve-discussion-paper-money-and-payments-in-the-digital-age/.

act as brokers themselves. Currently, large data sets of credit and debit card transactions are available for purchase to almost anyone. A search on the bulk dataset aggregator Datarade returned 35 separate datasets offering individual credit or debit card transactions for sale, and 234 total data sets offering transaction data including bank-to-bank transactions, electronic payment transactions, and loyalty card data.[6] The widespread dissemination of this data poses substantial privacy risks because this type of transaction data is easy to de-anonymize. In 2015 a study found that metadata from just four transactions in a dataset was enough to identify the cardholder in 90% of cases.[7] Current payment systems are designed to enable data brokers to collect, aggregate, and sell consumer data, and we do not have legal or regulatory privacy protections to prevent abuse.

The widespread brokering of financial transaction data can cause substantial harms to individuals. Brokers that collect or purchase transaction data can use it to build detailed profiles of individuals that can reveal or be used to infer private information about them, including their political views, their religious beliefs, their reproductive and family choices, and their personal preferences and habits. These data can also be used to underpin consequential decisions about where an individual can work, live, or even what price or level of service they receive. This pervasive profiling forces individuals into a "scored society" that frequently operates as a black box where they do not have access to the most basic information on how they are evaluated. Secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs. (For more information on black box algorithms, see the work of Frank Pasquale.)[8] And many times, algorithmic scoring does not create rational results. In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate

[6] Datarade, *Best Transaction Datasets*, https://datarade.ai/data-categories/transaction-data (2023).
[7] John Bohannon, *Credit card study blows holes in anonymity*, Science (Jan. 30, 2015), https://www.science.org/doi/full/10.1126/science.347.6221.468.
[8] *See*, Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015), Frank Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (2020).

information about his mortgage.[9] For more information see: EPIC, *Data Brokers*,[10] and EPIC, *Screening and Scoring*.[11]

The widespread collection and use of transaction data also exacerbates risks of overbroad government surveillance. Law enforcement agencies have reportedly begun to purchase bulk data from brokers in ways that can sidestep constitutional and statutory privacy protections. For example, Immigrations and Customs Enforcement (ICE) uses transaction data from utility payments to identify allegedly undocumented individuals for arrest and deportation, even when those individuals live in "sanctuary cities" that have opted not to provide information to the agency.[12] Some of the data used by ICE uses was collected by credit reporting agency Equifax from another data broker holding more than 400 million utility records.[13] For more on ICE's access to private data, see Dana Khabbaz, *DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information*, EPIC (Aug. 2022).[14] Federal agencies have also had real-time access to credit card transaction data since at least 2010, creating risks of oversurveillance, wrongful arrest, and abuse.[15] Access to credit card data can be obtained without a warrant.

The current digital payments landscape is over-surveilled and under-regulated. Individuals are subject to private and corporate surveillance from payment services providers and data brokers. That data is used to monitor, evaluate, and score individuals through opaque algorithms, eliminating

[9] Barry Ritholtz, *Where's the Note? Leads BAC to Ding Credit Score*, ritholtz.com (Dec. 14, 2010), https://ritholtz.com/2010/12/note-bac-credit-score/.
[10] https://epic.org/issues/consumer-privacy/data-brokers/.
[11] https://epic.org/issues/ai/screening-scoring/.
[12] Georgetown Center on Privacy and Technology, *American Dragnet, Data-Driven Deportation in the 21st Century* (May 10, 2022), https://americandragnet.org/finding3.
[13] *Id*.
[14] https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/.
[15] Ryan Singel, *Feds Warrantlessly Tracking Americans' Credit Cards in Real Time*, Wired (Dec. 2, 2010), https://www.wired.com/2010/12/realtime/?utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+Index+3+%28Top+Stories+2%29%29&utm_medium=feed&utm_source=feedburner.

financial privacy and harming individuals' access to credit, housing, and jobs. Much of the same data is available to law enforcement with little oversight or protections against misuse. A central bank digital currency could improve the current state of financial privacy, but only if carefully designed to preserve privacy and minimize surveillance.

II. Digital wallets create under-studied risks of theft and privacy harms.

In response to Question 2: Goals, sectors, or applications where digital assets introduces risks or harms:

There are substantial risks posed by intermediary and third-party implementation of digital wallets. Recent developments in the fintech and cryptocurrency ecosystem have shown that wallet services pose potentially substantial risks of data abuse, fraud, and other unfair practices if not adequately regulated. Malicious or improperly vetted wallet systems can exacerbate the problems of data aggregation, financial surveillance, and fraud. Implementing any new technology creates risks during the adoption period, when individuals are especially vulnerable to fraud and exploitation. And digital wallets pose unique risks because they expose individuals to commercial exploitation of personal transaction data as well as the risk of malicious third-party fraud, theft, or manipulation.

Without close review prior to deployment and constant scrutiny following adoption, the software and systems used to facilitate payments via CBDCs could cause more harm than good. Rampant theft and fraud in digital assets including cryptocurrency and Non-Fungible Tokens (NFTs) demonstrate the risks to consumers in implementing new and unregulated financial technologies. Digital wallets are currently used in cryptocurrency marketplaces, and associated transactions like

the sale of NFTs. A recent study from Chainalysis found that more than $3.2 billion in cryptocurrency was stolen in 2021, with the trend accelerating in 2022.[16]

While most of the largest thefts are accomplished by hacking cryptocurrency platforms, individuals are also widely vulnerable to fraud and theft. For example, in May 2022, hackers were able to spread fraudulent links across several popular NFT Discord channels, triggering automatic transfer of NFTs from unwitting users' digital wallets.[17] These thefts take advantage of individuals unaware of how easily current digital wallets can be exploited. Expanding digital wallet use across the economy by adopting a CBDC will expose even more vulnerable individuals to potential thefts and fraud. Digital wallets then present serious security risks that need to be addressed before widespread adoption, especially if they are to hold CBDC funds.

Digital wallets will have access to sensitive information and digital transactions, which inherently create detailed records unless designed to avoid them. Wallet apps will have access to users' personal information, banking information, and unless regulated could easily access phone location information as well.[18] Because digital wallets will have to interact with both banks and point-of-sale devices, the wallet is a potential privacy vulnerability as the app could collect information on both sides of a transaction. Unscrupulous wallet developers will have a strong incentive to design wallets that maximize data collection and make that data available for sale to data

[16] *Defi Hacks Are on the Rise*, Chainalysis (Apr. 14, 2022), https://blog.chainalysis.com/reports/2022-defi-hacks/.
[17] Lorenzo Franceschi-Bicchierai, *Hackers Compromise a String of NFT Discord Channels*, Vice (May 18, 2022), https://www.vice.com/en/article/k7wmpy/hackers-compromise-a-string-of-nft-discord-channels.
[18] *See, e.g.*, Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

brokers. And similar risks exist for point-of-sale systems, which will only provide transaction privacy if they are designed to do so.

New laws, regulations, and thorough product-testing are necessary to protect privacy for digital currency transactions. OSTP should invest in a government-vetted secure digital wallet and develop principles for data protection that should be in place before any government use of digital assets. The following principles are a starting point:

- **Data Minimization**: digital wallet providers should be prohibited from collecting any data that is not strictly necessary to make the digital wallet work;
  - **No Transaction Records**: digital wallet providers should not be permitted to create and maintain records of transactions conducted using the wallet;
  - **No Location Data**: digital wallets should not be permitted to collect or store location data or to transmit it off the device holding the wallet;
  - **No Data Exploitation**: digital wallet providers should not be permitted to sell or transfer data collected from wallet users;
- **Regulation**: Congress should designate one agency to implement regulations for digital wallets;
- **Product Testing**: Congress should mandate that either the National Institute of Standards and Technology or a designated regulatory agency perform rigorous product tests on all digital wallet apps to ensure that the apps conform with the above principles.

III. OSTP should prioritize a token-based CBDC that facilitates private payments to address some of the privacy harms in the digital payments space.

In response to Question 4: R&D that should be prioritized for digital assets.

Research into a digital currency presents a wide array of models. Any research should at least equally invest in a currency that uses a token-based system that does not rely on distributed ledger technology. The Fed should look to the work of cryptography and digital cash pioneer David Chaum for guidance in implementing a token-based CBDC.

A token-based digital currency issued by the Federal Reserve would present several advantages. First, a token issued by the Federal Reserve could be incorporated into the current banking system, making it easier to adopt as a CBDC. Second, it is possible to design a token that replicates the transaction privacy created by physical cash but also implements anti-money

laundering protections.[19] This type of CBDC would be a substantial improvement for consumer privacy as payment service providers would not be able to exploit transaction data. Third, by avoiding a distributed ledger system, a token issued by the Federal Reserve would have affordable transaction costs and be easy to scale up for public use.[20] Fourth, tokens can be designed to expire and need to be refreshed after a certain amount of time, cutting down on currency hoarding and reducing the ability of a central bank to do long term financial surveillance. Expiration dates can ensure that a CBDC is mainly used for transactions.

A token-based CBDC could work with existing intermediaries (banks) and would be able to preserve transaction privacy while allowing for anti-money laundering controls. To accomplish this, currency in the form of tokens would be issued by a central bank, transmitted to users through commercial banks, and encrypted and stored in a digital wallet. To spend the token, the user transmits it to a merchant, who deposits it with the merchant's bank and then the central bank to verify it has not been used before ("double spent"). Using a public/private key pair, merchants can verify the validity of the token using the central bank's public key, but would not receive the payer's private key, maintaining payer anonymity. Similarly, because neither the commercial bank nor the central bank can see the token's unique identifier, a merchant depositing the coin with the central bank does not reveal the individual who withdrew it. Banks would still be able to implement anti-money laundering controls because merchants are identified and verified when their accounts are created. By limiting the amount of currency a merchant can receive in one transaction, and monitoring patterns of payment with merchants, banks and the central bank can conduct strong anti-money laundering activities without compromising privacy for payers.

[19] *See* Chaum 2021 at 12-13.
[20] *Id* at 3.

OSTP should look to the work to David Chaum to design a CBDC that improves privacy for digital transactions. The following publications are particularly relevant:

- David Chaum, Christian Grothoff, Thomas Moser, *How to issue a central bank digital currency*, Schweizerische Nat. Bank (Mar. 2021), https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf.

- David Chaum, Amos Fiat, and Moni Naor, *Untraceable Electronic Cash (extended abstract)*, Advances in Cryptology CRYPTO '88, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327, https://chaum.com/wp-content/uploads/2021/12/Untraceable_Electronic_Cash.pdf.

- David Chaum, *Privacy Protected Payments Unconditional Payer and/or Payee Untraceability*, SMART CARD 2000, https://chaum.com/wp-content/uploads/2022/02/Privacy-protected-payments-unconditioanal....pdf.

For work specifically on how anonymous digital currencies can comply with anti-money laundering controls we recommend the following articles by cryptography and anonymous credentials pioneer Anna Lysyanskaya:

- Jan Camenisch, Susan Hohenberger & Anna Lysyanskaya, *Balancing Accountability and Privacy Using E-Cash (Extended Abstract)*, 4116 Security and Cryptography for Networks 144-55 (2006), https://link.springer.com/chapter/10.1007/11832072_10.

- Markulf Kohlweiss, Anna Lysyanskaya & An Nguyen, *Privacy-Preserving Blueprints*, Cryptology ePrint (Nov. 6, 2022), https://eprint.iacr.org/2022/1536.

In addition, OSTP should investigate fully anonymous digital currency and present fully anonymous currency as an option in future research and publications. Developing a digital currency will be a long-term process that presents the opportunity to re-think the costs and benefits of anti-money laundering laws. Fully anonymous digital cash may present even greater benefits to privacy, consumer protection, and inclusion for currently unbanked individuals that should be explored. And the use of intermediaries to facilitate the use of CBDCs should make it possible to integrate an anonymous digital payment mechanism through the intermediary while complying with anti-money laundering and fraud regulations as the current system already does with cash deposits and

withdrawals. OSTP should investigate and provide an option for fully anonymous digital cash to inform the discussion around CBDC design and allow the public to weigh in on whether a fully anonymous digital currency is desirable.

IV. OSTP should prioritize research into fully anonymous credentials.

In response to Question 4: R&D that should be prioritized for digital assets.

Anonymous credentials offer a way to verify whether a person has the authority to access a space or engage in a transaction without revealing anything about that person's identity. Anonymous credentials would prevent the process of verification from leaving behind a persistent identifier that would allow a payment collector, the government, or a bad actor to link a single instance payment or identity verification to other instances, preventing the accumulation of transaction data. Anonymous credentials will have a substantial role to play in preserving privacy in an increasingly digital world by reducing the information exposed to facilitate transactions. Digital assets, particularly if implemented in a widespread manner like a CBDC, could either improve the current state of financial privacy or make a bad situation even worse. Both the technology behind anonymous credentials and the system design required to use them have a broad overlap with digital assets. Advancing research into anonymous credentials then is a key step towards a privacy-preserving digital payment space.

For more on anonymous credentials, we recommend the work of Anna Lysyanskaya.

- Anna Lysyanskya, Signature schemes and applications to cryptographic protocol design (2002), https://dspace.mit.edu/handle/1721.1/29271
- Melissa Chase, *Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications* (May 2008), http://static.cs.brown.edu/research/pubs/theses/phd/2008/chase.pdf
- Fonteini Baldimtsi, *Efficient Cryptography for Information Privacy* (May 2014), https://cs.brown.edu/research/pubs/theses/phd/2014/baldimtsi.pdf

- Endre Bangerter, Jan Camenisch, Anna Lysyanskaya, A Cryptographic Framework for the Controlled Release of Certified Data, 3957 LNCS 20-42 (2006), https://link.springer.com/chapter/10.1007%2F11861386_4.

V. Conclusion

EPIC urges OSTP to foreground privacy and consumer protection as key considerations in its review of digital currency and digital assets. Because a digital currency by itself will not solve equity, privacy, and fraud harms, the government should move slowly to ensure that it does not adopt or encourage use of systems that pose new and significant risks. As part of that review, agencies should undertake a closer review of current data collection and use practices within the digital payment ecosystem and consider the need for greater privacy protections. OSTP should consider a fully anonymous digital cash option for the CBDC, and at a minimum should look towards a token-based CBDC that improves privacy in digital transactions from the status quo.

OSTP can promote responsible digital asset development by investing in research into anonymous digital cash, an intermediated CBDC with privacy-preserving anti-money laundering controls, and anonymous credentials. We also urge OSTP and any policymakers not to ignore the substantial privacy and security risks posed by unvetted and unregulated digital wallets. For further questions, please contact EPIC Counsel Jake Wiener at wiener@epic.org.

Respectfully Submitted,

/s/ John Davisson
John Davisson
EPIC Senior Counsel &
Director of Litigation

/s/ Jake Wiener
Jake Wiener
EPIC Counsel