Kafka's Wallet: Building Trust Despite Financial Surveillance in CBDCs

Kyle Beadle *Advisor: Dr. Marie Vasek*

Department of Computer Science
University College London
kyle.beadle.22@ucl.ac.uk

Abstract

As central bank digital currencies (CBDC) are increasingly developed, piloted, and launched around the world, central bankers have begun to worry about consumer adoption. Privacy concerns remain a common critique of CBDCs and poses a serious challenge for adoption as consumers worry about third-party data brokers, data breaches and government surveillance. Therefore, we develop a framework, derived from surveillance studies, to conceptualize how central banks current conceptions of privacy facilitate unregulated consumer monitoring. We then evaluate three central bank's digital currency pilot programs, Canada, Japan, and Sweden, towards comparing their different approaches to privacy. We find that while all three central banks considered privacy to be a fundamental feature of CBDCs, they all fail to thoroughly address issues surrounding the processing and retention of customer data. Finally, we discuss the implications of our findings for gaining consumer trust in CBDCs. We propose a future research agenda for further CBDC development and argue that central banks need to balance national security and privacy.

Threat: Data Breaches

Cybercriminals claim hack of EU police agency, posting data online

Sensitive data from the EU's police agency appeared for sale on a cybercrime forum.

▷ LISTEN SHARE

POLITICOPRO Free article usually reserved for subscribers

EU law enforcement agency Europol suffered a recent data breach in which hackers infiltrated internal platforms. | Jasper Jacobs/AFP via Getty Images

Figure: https://bit.ly/4daqBmr

Threat: Data Brokers

European data broker

Sensitive passport data of Germans published online

A data broker is offering sensitive passport data of thousands of people for sale – and publishing some of it openly online. Our investigation leads to an airline as a possible source. Data protection authorities are alarmed.

25.04.2024 um 12:24 Uhr - Chris Köver, Sebastian Meineck, Ingo Dachwitz, Markus Reuter - in Datenschutz - eine Ergänzung

– Public Domain DALL-E-4 („a plane and a personal ID, bauhaus style reduced minimalist geometric shape"); Bearbeitung: netzpolitik.org

Figure: https://bit.ly/47vkF6y

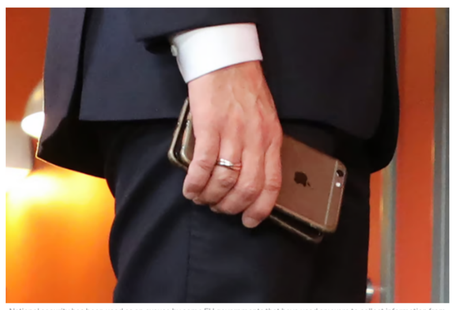
Threat: Government Surveillance

Curb your snooping, Commission tells EU governments

The EU executive tells member countries national security isn't a blank check to justify spyware use.

▷ LISTEN SHARE

POLITICOPRO Free article usually reserved for subscribers



National security has been used as an excuse by some EU governments that have used spyware to collect information from phones and other devices belonging to lawyers, journalists and even opposition politicians. | Ludovic Marin/AFP via Getty Images

Figure: https://bit.ly/3TzGVq3

Results - Summary

Property	Canada	Japan	Sweden
Privacy commitment	●	●	●
Transparency	●	●	●
Accountability	◑	◑	◑
Regulatory compliance	◑	◑	◑
Context-specific regulation	◑	◑	◑
Privacy enhancing technologies	●	●	●
Data retention scheme	○	○	○
Data access scheme	○	○	○
Maintenance	●	●	●
Exceptions	○	○	○

● = Fully present
◑ = Partially present
○ = Not present

Results - Sweden

The rapidly evolving digital world is also highly relevant for the process of regulating private forms of money. Such regulations necessarily involve tradeoffs between specificity and flexibility. Specific regulations can help protect the public interest but may require frequent revision to reflect changes in technology, facilitate transparency and efficiency, and ensure broad compliance by regulated firms. Indeed, these issues are likely to be acute in the context of overseeing huge multinational enterprises and global payment networks. Such revision takes considerable time and, by the time the revisions are ready to be implemented, there is considerable risk that they will no longer be adequate for the situation for which they were devised. A direct government presence in the payment market in the future, through an e-krona, could therefore potentially be a *more adaptable* instrument than regulation, or a good complement to regulation, to handle ongoing changes.

Figure: https://bit.ly/3MMw7RD

Results - Canada

Privacy

Enabling both privacy and regulatory compliance will be challenging, but new technologies provide options. 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). While not every possible requirement will be practical, new cryptographic techniques may allow the Bank to satisfy the need for privacy as well as controlled disclosure (e.g., disclosure required to comply with anti-money laundering regulations).

Figure: https://bit.ly/4e7VkCe

Results - Japan

Regarding "overlay services," information is transferred only between the private service providers and the users. The central bank is not in a position to obtain or utilize the user's transaction information. For the private service providers, the information provided by users can be a source of new services and businesses. From the perspective of user convenience and adding value of overlay services, how the private sector can effectively utilize user information will be an issue to be considered due course.

Figure: https://bit.ly/4e2LNMt

Conclusion

- Technical solutions alone will not build trust in CBDCs.
- Data from CBDCs can be used to combat financial crime and protect national security, but it is important to issue assurances against surveillance creep.
- Additional research is needed to understand the global landscape of privacy in ongoing CBDC programs.
- Future developments from central banks should focus on increasing accountability measures and auditing the data access and retention schemes.
- Future policy solutions should tackle financial surveillance specifically and outline how central banks should handle national security exceptions.

Engineering and Physical Sciences Research Council