Using Contextual Integrity to Uncover Acceptability of Information Flows in Central Bank Digital Currency Transactions

Frédéric Tronnier
Goethe University Frankfurt,
Germany
frederic.tronnier@m-chair.de

Abstract

Central Bank Digital Currency (CBDC) are a rapidly evolving payment technology, with privacy being a crucial factor. Research on privacy in CBDC is limited and focuses mainly on technical considerations and its link to adoption intention. This paper presents a first step towards understanding privacy norms in digital euro transactions for German citizens. The study employs a large-scale questionnaire, based on contextual integrity theory, to investigate acceptable flows of information and privacy parameters for CBDC and other digital payment methods. We conduct a pretest with 127 respondents, followed by a main study with 1064 respondents to measure and compare acceptability of various information flows. The results reveal the importance of (un)acceptable recipients of transaction- and identity-related information and the influence of different transmission principles. The findings can be used by central banks and policymakers to design and implement CBDC that corresponds to individuals' privacy norms.

Keywords: Contextual Integrity, Central Bank Digital Currency, Digital Euro, Privacy Concerns, Electronic Payments

1. Introduction

Money has undergone significant evolutionary steps throughout history, starting with physical coins and paper-based banknotes to credit cards and digital payment solutions. The emergence of blockchain-based cryptocurrencies, particularly stablecoins, is being considered a potential next step towards future payment methods (European Central Bank, 2020). Additional events such as the COVID-19 pandemic intensified the demand for new monetary solutions by decreasing the use of cash by individuals (Dionysopoulos et al., 2023). Central banks now needed to react to the new challenges of a decrease in cash use and the emergence of (de)centralized cryptocurrencies (Kosse & Mattei, 2023; Dionysopoulos et al., 2023). The proposed solution is the creation and issuance of Central Bank Digital Currencies (CBDC), to foster financial inclusion and increase payment efficiency, with 93% of all surveyed central banks researching, working or piloting CBDC (Kosse & Mattei, 2023). The European Central Bank (ECB) is actively exploring the introduction of a digital euro and conducted a survey to gauge stakeholders' perceptions of such a CBDC. The results revealed that EU citizens expressed a clear preference for a privacy-sensitive, and secure, solution (European Central Bank, 2021). The ECB's objective with a digital euro is to retain trust in central banks and central bank money, within the digital age (European Central Bank, 2021). While the eventual design of the digital euro is still unknown, the ECB aims for the digital euro to function as a digital representation of the existing euro, to be used alongside cash. It is intended to facilitate retail transactions for citizens, exhibiting features reminiscent of cash (European Central Bank, 2020).

As the public consultation on the digital euro demonstrated privacy to be the most important factor for end-users (European Central Bank, 2021) research is now investigating this factor in detail. In a working paper by David Chaum, the creator of eCash, of the Swiss National Bank, the potential for mass surveillance through CBDC is noted (Chaum et al., 2021). Indeed, privacy concerns in CBDC are found to decrease adoption intention (Tronnier et al., 2022), a finding that aligns with prior research on other digital payment solutions (Reith et al., 2020). For blockchain-based CBDC, there exist first proposals for privacy-sensitive solutions, using Zero-Knowledge-Proofs (ZKP) (Gross et al., 2021). What is more, privacy is also increasingly being researched for already existing, and widely-used, digital payment methods (Sahi et al., 2022) for instance in the e-commerce context (Bandara et al., 2020).

While it could be demonstrated that individuals do exhibit privacy concerns for CBDC payments (Tronnier et al., 2022), it is not apparent what it is exactly that

URI: https://hdl.handle.net/10125/107093
978-0-9981331-7-1

concerns them, and whether and how those concerns differ from concerns when using existing digital payment solutions. We therefore aim to uncover whether and how individuals' perceptions of privacy differ between existing digital payment methods and future CBDC transactions. Contextual integrity (CI) theory by Nissenbaum (2009) argues that privacy, and perceived privacy violations, are context-dependent. We therefore employ CI theory with the aim to study differences in CI parameters between CBDC and existing payment methods. The overall goal is to provide a first step towards uncovering inherent privacy norms in CBDC payments that are likely to be paramount in ensuring CBDC adoption in the future.

To this end, we employ the survey method by Apthorpe et al., (2018) and contextual integrity (CI) theory by Nissenbaum (2009) to study the acceptability of flows of information in different digital payment transactions. We thereby address the following research questions:

RQ1: Which flows of information are regarded as appropriate in digital euro transactions?

RQ2: How do digital payment methods differ in terms of appropriate flows of information for individuals?

To our knowledge, no previous research has applied CI towards digital payment methods. We therefore employ a quantitative approach to study and compare acceptable flows of information between three types of digital payments, namely traditional Online Banking, PayPal and digital euro transactions. We conduct a pretest with 127 respondents to develop and refine CI parameters. The main survey consists of 1064 German-speaking respondents across the three payment solutions.

2. Background and Related Work

2.1. CBDC and the Digital Euro

To define CBDC and to distinguish it from existing types of money, it is advisable to define money first. Ideally, any type of money should fulfill three core properties, that are (1) to act as a unit of account and (2) a medium of exchange as well as (3) to be a store of value. Money can be characterized based on four key properties, the issuer, form, accessibility, and technology employed (Tronnier et al., 2023). The issuer can be a central bank or private banks, money can exist in digital or physical form, and it may be accessible to the general public or limited to interbank transactions. Additionally, money can be account-based or token/value-based when employing distributed ledgers or blockchain technology (Bech & Garratt, 2017). Presently, central banks issue only banknotes (and coins) as legal tender for the general public.

CBDC is therefore central bank-created, digital currency that may be designed for wholesale, interbank, purposes or to as a retail solution, for the public. From a technology perspective, blockchain and account-based solutions are presently being researched (Bech & Garratt, 2017). As this definition is rather broad, this work focuses on one specific CBDC, namely the digital euro, as defined by the ECB. The digital euro is currently expected to be a retail CBDC, to be used by individuals for public use, with the underlying technology yet to be determined. The digital euro is not intended to replace cash, but rather to complement it for online payments (European Central Bank, 2022) Its objectives are threefold: (1) to maintain trust in the euro as the primary monetary anchor in Europe, (2) to provide citizens with a secure and risk-free digital payment alternative not offered by the private sector, and (3) to prevent domination of the payment sector by non-European organizations that may prioritize their own interests over that of citizens and countries (Lagarde & Panetta, 2021).

Researchers and central bankers have discussed the potential benefits and threats of CBDC. Advantages include the potential for increased payment efficiency, financial stability and inclusion, as well as improved anti-money laundering capabilities (Schueffel, 2023). For individuals, the benefits of CBDC are less apparent, in particular given potential privacy and surveillance concerns at an individual and societal level (Schueffel, 2023). First research on CBDC adoption intention indicates that established factors such as performance expectancy, social recommendations and facilitation conditions (Solberg Söilen & Benhayoun, 2022) as well as trust and privacy protection (Tronnier et al., 2022) are crucial. Additionally, recent research highlights the interrelatedness between CBDC and other payment methods from a users' perspective (Tronnier et al., 2023). The authors find that attitudes towards unfamiliar CBDC are influenced by the perceived equivalence of the CBDC to existing, familiar payment methods.

With research on CBDC increasing exponentially, the topic of privacy is also being covered by central banks and academics, with a mapping of the privacy landscape provided by Auer et al. (2023) and a taxonomy of technical approaches towards privacy in blockchain-based CBDC by Lee et al. (2021). From an economics perspective, Fang et al. (2023) utilize game theory to establish the need for a balanced approach towards privacy protection and regulation, while also promoting user education on the subject. Different technical and conceptual approaches towards implementing privacy are already being studied (Dogan & Bicakci, 2023 using techniques such as Zero-

Knowledge Proofs (Gross et al., 2021). Other research uses privacy calculus theory and finds that significant benefits offset privacy concerns in information disclosure in CBDC (Jabbar et al., 2023) or study antecedents influencing privacy concerns in CBDC (Tronnier & Biker, 2022).

2.2. Privacy and Contextual Integrity

Apart from its three core functions, digital payment methods also act as a store of information, as digital transactions process different types and amounts of information. Transaction data is routinely processed to comply with regulation and anti-money laundering (AML) and/or know-your-customer (KYC) regulation, which is likely to be also the case for CBDC transactions (Wadsworth, 2018). Personal data could therefore be revealed during the transfer of CBDC transaction-level financial information (Auer & Böhme, 2020), with CBDC at risk of "becoming a digital leviathan" that threatens privacy and the erosion of civil liberties (Baronchelli et al., 2022). The protection of privacy is a fundamental human right and regulated through various legislations, for instance through the General Data Protection Regulation (GDPR) in Europe. Protecting privacy is therefore not only useful to mitigate privacy concerns, which hinder CBDC adoption (Tronnier et al., 2022), and negatively influence digital payment and cryptocurrency usage (Hamm, 2022; Reith et al., 2020), but also necessary to ensure regulatory compliance.

The theory of contextual integrity (CI) (Nissenbaum, 2009) states that expectations and perceived violations of privacy are context-dependent; the flow of information between entities needs to be appropriate. This appropriateness is based on "behavior-guiding norms [that] prescribe and proscribe acceptable actions and practices" (Nissenbaum, 2009). A specific flow of information, that violates privacy norms is deemed inappropriate and can lead to privacy concerns. Inherent privacy norms and appropriate flows of information can be uncovered through the combination of five key CI parameters: subject, sender, recipient, information type and transmission principle (Nissenbaum, 2009). Using these parameters, individuals' expectations, perceived privacy violations and inherent norms can be uncovered systematically (Nissenbaum, 2009). A context-dependent information flow that violates privacy norms might be deemed inappropriate by an individual, which results in privacy concerns. As an example, the author describes that the use of health-related data (*information type*), given to a doctor (*recipient*) by a patient (*sender* and *data subject*) is likely to be deemed appropriate if the data is to be used to find a cure for a disease (*transmission principle*). In contrast, the same flow could be deemed inappropriate, by the data subject, if a doctor uses the data for advertising purposes, as the transmission principle was changed.

While there exists research on using CI and CI parameters in other contexts, for instance for privacy policies (Shvartzshnaider et al., 2018) or smart home devices (Apthorpe et al., 2018), no research has been conducted on CI for digital payment solutions and CBDC. There exist research that identifies or relates to specific CI parameters in the context of digital payments. For instance, it was found that US citizens dislike the disclosure of contact information, e.g., mail or home address, to merchants (Hoofnagle et al., 2012). The recent work of Dogan & Bicakci (2023) also relates to the topic in that the authors remark that privacy conflicts in CBDC not only arise between users and regulatory authorities but also between users and banks. The authors provide a ledger-based solution that hides information on senders and recipients, if desired. For CBDC transactions, possible processed data is categorized into identity-related or transaction-related information (Allen et al., 2020; Lee et al., 2021).

3. Methodology

We employ a quantitative approach to study individuals' attitudes towards information flows in different digital payment methods in order to compare them. Our research design follows the survey method by Apthorpe et al. (2018) who state that "information flows and associated contexts can be described using five parameters: sender, recipient, subject, attribute, and transmission principle. This precise formulation makes it possible to thoroughly investigate the combinatorial space of contextual information flows and associated privacy norms" (Apthorpe et al., 2018). We therefore adapt the authors' survey framework towards CBDC.

3.1. Identification of CI Parameters

As little is known on the specifics of most CBDC, it is necessary to make assumptions on the possible design of a CBDC and the corresponding information flows during a transaction. Thus, this work focuses solely on the digital euro, as outlined by the ECB for the Euro Area (European Central Bank, 2021). The ECB communicates objectives and design options transparently and already published research on the importance of privacy for surveyed end-users (Eurogroup, 2022). Moreover, the different design options, technical implementations and objectives of different central banks make it necessary to decide for one focus group, German citizens. Auer & Böhme (2020) map consumer needs for CBDC onto design choices and outline potential retail CBDC architectures.

The digital euro is therefore presented to respondents in the survey as an indirect CBDC, designed to be accessible to all citizens as a convenient alternative to cash for digital transactions. In the following, we describe the CI parameters that are utilized in this study:

Sender and Data Subject: For all payment methods, sender and data subject are the individuals and citizens in the Euro area that conduct digital payments.

Recipient: There exist countless potential recipients of data in digital payments. To limit the number of recipients for this work, we include the central bank (ECB), the respondents' house or retail bank, the government, and other payment service providers (PSPs), whereby ApplePay was given as an example in the survey. All other possible recipients, such as advertisers, data aggregators, were tested for in the pretest and later summarized as third parties in the main study. This was done as the pretest indicated that respondents' attitudes did not differ significantly between several third parties.

Information Type: Following academic literature, information type are clustered into identity-related and transaction-related information (Allen et al., 2020; Lee et al., 2021). Examples for both types are outlined in the questionnaire, e.g., transaction amount, time, location and product type for transaction information and data subjects' age, gender and address for identity-related information. We decided on these two types to reduce the number of possible combinations for the main study and to cognitive overload for participants.

Transmission Principles: Principles are obtained through existing research on CI parameters that involve data sharing (Apthorpe et al., 2018) and through information published by central banks and payment-related institutions (Eurogroup, 2022). For instance, researchers argued that low value CBDC transactions, e.g., with a value of less than €100, could be conducted anonymously, while higher value transactions would need to be monitored (Lee et al., 2021). We tested several transmission principles using the pretest and opted to include nine principles in the main survey. These include the use of data for advertising, for the prevention of illegal activities (Eurogroup, 2022) and for the improvement of a recipients' services.

3.2. Questionnaire Design

The main study consists of three questionnaires that survey average acceptability scores of different flows of information for (1) digital euro, (2) PayPal and (3) Online Banking transactions as we not only want to evaluate the acceptability of CBDC information flows but want to also compare them to existing payment solutions. PayPal and Online Banking were chosen as PayPal is found to be the most accepted payment method for B2C E-Commerce (Coppola, 2023) with 93.6% acceptance rate and 78% of German citizens having used Online Banking solutions with their bank (Bitkom, 2023). All three surveys followed the same layout and used the same wording, if possible, in their items. The survey consisted of five pages of questions and an introductory page that provided information on the objective of the study, the main author, as well as the necessary information on data collection objectives and survey length. The last page included demographic questions and was identical for all three groups.

Introductory Information: An introductory text on either the digital euro, PayPal and Online Banking was given on the first page of the questionnaire. The introductory text was based on the ECBs most recent information on the digital euro. The introductory texts for the other payment methods followed the one on the digital euro in terms of language and text length to increase comparability. In the pretest, respondents were questioned on their understanding of the digital euro and its differences to cash and other digital payment methods. To ensure that participants understood the introductory information, we evaluated readability by calculating Flesch Reading Ease and Flesch-Kincaid Grade Level tests. Flesch Reading Ease was 49.8/32.7/39 for the introductory texts on the digital euro/PayPal/Online Banking. Flesh-Kincaid Grade Levels were 9.5/12/11.6 respectively, indicating a college reading level. Following the pretest, we adopted various changes for the main study. We refined the introductory text on the digital euro using new information by the ECB, although the pretest confirmed the information to be of high understandability.

Contextual Integrity Questions: The main part of the surveys consists of multiple question matrixes in which 5-point Likert scales are used to evaluate average Likert acceptability score (AAS), following the item design of Apthorpe et al. (2018), of different flows of information, for all three payment types. An example of such a matrix is given in **Figure 1** that depicts only part of the 5-point Likert scale due to lack of space.

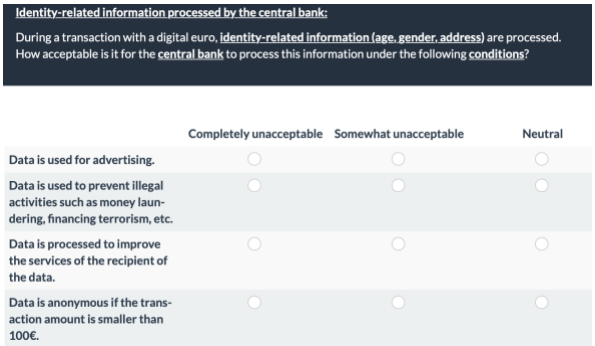

Figure 1. Exemplary digital euro transaction matrix with differing transmission principles

Here, respondents were asked how acceptable they would find if a specific *information type* would be transferred to a specific *recipient*, under a specific *transmission principle*, in future digital euro transactions. The English pretest only surveyed AAS for the digital euro, in order to test for understandability and to gather suitable transmission principles and recipients. The main study repeated the process also for PayPal and Online Banking transactions and was available in English and German, with items being translated back and forth by several researchers to ensure consistent meaning between languages. We first surveyed AAS for the combination of all recipients and all information types without transmission principles, followed by all combinations including the nine transmission principles. This resulted in a total of 12 sets of matrix questions with a total of 110 items for each participant of one of the three payment technologies. The AAS are tested for significant difference between information types using pairwise t-tests and Cohen d values.

3.3. Participants and Ethical Considerations

This study focuses on the German population, as German individuals were found to demonstrate the highest preference for privacy in a digital euro across European countries (European Central Bank, 2020). Focusing on one country also allows controlling for the influence of nationality and culture, factors identified in established research to influence privacy concerns (Smith et al., 2011). The pretest was conducted anonymously using LimeSurvey, with respondents collected through word-of-mouth, social media channels and university lectures. Participants were not limited to a specific country and the pretest could be taken in both, German and English.

For the main study, participants were recruited through a professional market research institute, bilendi.com, certified by ISO 20252:2019. Participation was limited to individuals with German as their first language. We used quotas to survey an equal number of male and female respondents. Participants were reimbursed for their work and randomly allocated towards one of the three surveys on either digital euro, PayPal or Online banking transactions. The study received exempt status from ethical review in accordance with the guidelines and the approval of our institutions' ethical commission.

4. Results

In the following, we jointly present the results for the pretest and the main study, starting with the descriptives before going into detail with AAS scores. Median response time for all main surveys was 9:35 minutes.

4.1. Descriptives

Table 1. Descriptives of the pretest and the main study

Questionnaire		**Pretest**		**Digital Euro**		**PayPal**		**Online Banking**	
		#	**%**	**#**	**%**	**#**	**%**	**#**	**%**
Gender	Male	76	59.84	177	49.72	178	50.14	178	50,42
	Female	47	37.00	177	49.72	177	49.86	175	49,58
	Other/No answer	4	3.15	2	0.56	0	0	0	0,00%
Age		M=40.4	SD=17.4	M=46.2	SD=14.2	M=45.6	SD=14.3	M=46.6	SD=13.9
	18 - 29	56	44.09	63	17.7	58	16.34	50	14.16
	30 - 31	8	6.30	62	17.42	79	22.25	74	20.96
	40 - 49	8	6.30	69	19.38	61	17.18	70	19.83
	50 - 59	31	24.41	74	20.79	77	21.69	76	21.53
	60+	23	18.11	86	24.16	78	21.97	81	22.95
	No answer	1	0.79	2	0.56	2	0.56	2	0.57
Degree	No school diploma	-		1	0.28	2	0.56	1	0.28
	Elementary school	-		40	11.24	44	12.39	28	7.93
	Secondary school	-		104	29.21	102	28.73	115	32.58
	A-levels	-		78	21.91	80	22.54	79	22.38
	Bachelor's degree	-		41	11.52	51	14.37	49	13.88

	Master`s degree	-		82	23.03	69	19.44	74	20.96
	PhD and higher	-		9	2.53	5	1.41	6	1.70
	No answer	-		1	0.28	2	0.56	1	0.28
Knowledge	Financial	35	27.1	48	13.48	44	12.39	36	10.2
	Technology	34	26.4	52	14.61	72	20.28	62	17.56
	Legal	29	22.5	29	8.15	26	7.32	26	7.37

The descriptives are presented in **Table 1**. The pretest consists of 127 final respondents, accounting for incomplete questionnaires, data cleansing and age. The majority of respondents had no relevant background knowledge. Following the introductory text, respondents stated that they understood the concept of the digital euro (M=1.09, SD=.88), understand how it differs from cash (M=1.35, SD=.93) and other digital payment methods (MN=1.05, SD=1.05), on a 5-point Likert scale from -2 to 2.

A total of 1064 respondents participated in the main study, randomly assigned to one of the three payment solutions and controlled for an equal number of male and female participants. With a mean age of 45 – 46, respondents are comparable between the three groups. The mean age of respondents is slightly higher than the mean age for German citizens, which is not surprising as respondents under 18 were not surveyed. Notably, the Online Banking group reports the highest number of respondents with self-described prior work experience, related to the IT-knowledge, while having the lowest number with regards to financial knowledge.

4.2. Average Acceptability Scores (AAS)

The pretest surveyed AAS for 12 recipients and ten transmission principles, which were then condensed to five recipients and nine transmission principles in the main study. The transfer of identity-related information to the retail bank is found to be regarded as the only, marginally, acceptable information flow. Transferring transaction-related information is generally considered to be less acceptable for most recipients. Several third parties, such as advertisers or social networks, are generally considered as unacceptable data recipients. We therefore omitted them in the main study as results would likely be similar and are not surprising, also considering related work (Apthorpe et al., 2018).

AAS scores of the main study for the combination of recipients and information types (without transmission principles) are depicted in **Table 2** as the baseline scenario, ranging from -2 (completely unacceptable) to +2 (completely acceptable). Significant difference (pairwise $p < .05$) between information types can be seen in particular for digital euro transactions. For all payment solutions, effects size is defined as small, with Cohen $d < 0.5$ (Cohen, 1988).

As also observed in the pretest, and for all payment solutions, only the transfers of transaction and identity-related information to the respondents' house bank are viewed as somewhat acceptable. Notably, the transfer of identity-related information is viewed as less acceptable than the transfer of transaction-related information, across all three payment solutions. Third parties and the government are regarded as the least acceptable recipients of data. **Table 3, Table 4, Table 5** now build upon the prior table and includes nine transmission principles. Bold values mark $p < .05$ for the comparisons of information types. Effect size Cohen d was low (< 0.5) for all of those comparisons.

Table 2. Average Acceptability Scores (AAS) for transaction-related (TI) and identity-related (II) Information. T= t-value, p = pairwise p, d= Cohen d

	AAS Digital Euro					**AAS PayPal**					**AAS Online Banking**				
Recipient	**TI**	**II**	**T**	**p.**	**d**	**TI**	**II**	**T**	**p.**	**d**	**TI**	**II**	**T**	**p.**	**d**
ECB	-0.28	-0.66	7.28	.00	0.39	-0.34	-0.51	3.57	.00	0.19	-0.25	-0.41	3.62	.00	0.19
House Bank	0.27	-0.08	6.66	.00	0.35	0.32	0.06	5.31	.00	0.28	0.69	0.33	6.29	.00	0.33
Government	-0.9	-1.01	3.06	.00	0.16	-0.82	-0.86	0.92	.39	0.05	-0.78	-0.77	-0.36	.71	-0.02
Other Payment Providers	-0.24	-0.6	6.93	.00	0.37	-0.52	-0.75	5.52	.00	0.29	-0.08	-0.42	6.88	.00	0.37
Third Parties	-0.98	-1.18	4.76	.00	0.25	-0.83	-0.92	2.20	.03	0.13	-1	-1.07	1.96	.05	0.10

Table 3. AAS for digital euro transactions across recipients, information types and principles.

Digital Euro | Recipient	Central Bank		House Bank		Government		Third Parties		Other PSPs	
Information Type	**II**	**TI**	**II**	**TI**	**II**	**TI**	**II**	**TI**	**II**	**TI**
Transmission Principle: Data ….										
used for advertising.	-1.21	-1,16	**-1,18**	**-1,08**	-1,24	-1,21	**-1,22**	**-1,19**	-1,18	-1,1
used to prevent illegal activities.	**0.12**	**0,27**	0,25	0,26	0,05	0,06	-0,37	-0,4	-0,13	-0,08
used to improve recipients' services.	-0.47	-0,44	-0,39	-0,42	-0,8	-0,75	-0,86	-0,81	-0,58	-0,58
anonymous if transaction < €100.	0.29	0,28	0,3	0,35	-0,07	-0,05	-0,31	-0,34	-0,02	-0,04
is anonymized.	0.76	0,69	0,65	0,65	0,27	0,25	0,01	-0,03	0,3	0,31
only processed by authorized parties.	0,18	0,19	0,22	0,26	-0,19	-0,17	-0,43	-0,44	-0,1	-0,04
used under data protection regulation.	0,39	0,37	0,39	0,43	-0,01	-0,03	-0,29	-0,29	0,08	0,1
used to generate insights for recipient.	**-0,77**	**-0,66**	-0,64	-0,6	**-0,8**	**-0,73**	-0,84	-0,82	-0,69	-0,63
remains in control of user.	0,9	0,85	0,79	0,84	0,48	0,48	0,22	0,28	0,6	0,55

Table 4. AAS for PayPal transactions across recipients, information types and transmission principles.

PayPal | Recipient	Central Bank		House Bank		Government		Third Parties		Other PSPs	
Information Type	**II**	**TI**	**II**	**TI**	**II**	**TI**	**II**	**TI**	**II**	**TI**
Transmission Principle: Data ….										
used for advertising.	-0,95	-0,97	**-0,95**	**-0,86**	-1,06	-1,02	-0,99	-0,95	-1,03	-1,03
used to prevent illegal activities.	**0,22**	**0,32**	0,38	0,46	0,12	0,06	**-0,18**	**-0,08**	-0,29	-0,26
used to improve recipients' services.	-0,24	-0,16	-0,14	-0,1	-0,6	-0,54	-0,59	-0,56	-0,7	-0,67
anonymous if transaction < €100.	0,51	0,51	0,47	0,51	0,06	0,01	-0,06	-0,03	-0,24	-0,25
is anonymized.	0,89	0,85	0,83	0,81	0,41	0,35	0,28	0,3	0,09	0,09
only processed by authorized parties.	0,47	0,42	0,52	0,44	0,01	0,08	-0,1	-0,11	-0,21	-0,22
used under data protection regulation.	0,59	0,54	0,59	0,65	0,16	0,17	0,04	0,02	-0,08	-0,06
used to generate insights for recipient.	**-0,49**	**-0,35**	-0,3	-0,3	-0,57	-0,51	-0,64	-0,61	-0,72	-0,7
remains in control of user.	1,11	1,03	1,01	0,98	0,71	0,66	0,55	0,6	0,49	0,51

Table 5. AAS for Online Banking transactions across recipients, information type and principles.

Online Banking | Recipient	Central Bank		House Bank		Government		Third Parties		Other PSPs	
Information Type	**II**	**TI**	**II**	**TI**	**II**	**TI**	**II**	**TI**	**II**	**TI**
Transmission Principle: Data ….										
used for advertising.	-1,13	-1,1	-1,02	-1,01	-1,16	-1,16	-1,07	-1,1	-1,16	-1,14
used to prevent illegal activities.	0,27	0,32	0,39	0,39	0,16	0,22	0,13	0,18	-0,22	-0,16
used to improve recipients' services.	-0,35	-0,32	-0,26	-0,29	-0,63	-0,56	-0,43	-0,42	-0,69	-0,69
anonymous if transaction < €100.	0,29	0,29	0,3	0,27	-0,01	0,04	0,1	0,13	-0,23	-0,16
is anonymized.	0,81	0,78	0,73	0,74	0,39	0,45	0,48	0,5	0,11	0,12
only processed by authorized parties.	0,46	0,48	0,48	0,5	0,07	0,14	0,21	0,21	-0,15	-0,11
used under data protection regulation.	0,61	0,55	**0,66**	**0,58**	0,21	0,27	**0,36**	**0,43**	0,03	0,01
used to generate insights for recipient.	-0,65	-0,57	-0,45	-0,41	-0,57	-0,57	-0,56	-0,54	-0,71	-0,72
remains in control of user.	1,09	1,01	1,04	1,02	0,72	0,77	0,85	0,87	**0,56**	**0,64**

5. Discussion

The results, without any transmission principles involved, demonstrate that a respondents' house bank is the only, somewhat, acceptable recipient of information in digital payment transactions across all three payment solutions. A significant difference, but low effect size, can be observed between the transferred information, with the usage of identity-related information being viewed as less acceptable than that of transaction-related information. This is particularly the case for the digital euro. This indicates that, while the information type does have an influence on acceptability, that the recipients themselves are of more importance to respondents. From a respondents' perspective, identity-related information such as age or name might indeed relate more strongly to them, and could be seen as rather sensitive, in contrast to transaction-related information whose value may not be directly apparent to a respondent. The pretest already indicated the importance of recipients and demonstrated that multiple entities, such as social networks or advertisers are seen as unacceptable data recipients, which were therefore grouped as third parties in the main study. To assess whether these findings are CBDC specific, we repeated the survey for PayPal and Online Banking transactions.

When transmission principles are added to the digital payment methods information flows, notable changes can be observed. Depending on the combination of a specific transmission principle and a specific recipient, information flows become strongly unacceptable on the one hand, or rather acceptable on the other hand, compared to the baseline without transmission principles. For instance, while the baseline scenario depicts central banks as somewhat unacceptable recipients, this assessment changes towards rather acceptable, if the communicated goal is to let the central bank use the data to prevent illegal activities. This can be observed for both information types and also for other "positive" transmission principles. Most notably, letting the user/individual remain "in control over one's data" demonstrates by far the strongest level of acceptability, even though how this control over the data could work in practice was not communicated. Auer et al. (2023) also argue that privacy concerns are highly context-dependent and discuss that, as a non-commercial entity, a central bank might have no incentive to use transaction data for monetary gains, even though the potential for mass surveillance has been mentioned in prior research (Dionysopoulos et al., 2023). At the same time, a central bank would become an attractive goal for hackers and other actors if it would store and process large amounts of CBDC-related information (Auer et al., 2023), which could provide an additional explanation for the low AAS for the central bank. Transmission principles that provide no benefits for the user/respondent are regarded as unacceptable, across all three payment solutions. Again, this is not surprising, although data is, of course, in practice often used to, for instance, improve a recipient's services. This can also be one purpose of data processing to which a user or customer of payment services agrees upon when using a banking-related service. Moreover, respondents seem to be aware of the trade-off between users' privacy and AML/KYC requirements of organizations. Preventing illegal activities is seen as an acceptable transmission principle among all payment types and data recipients, except for undisclosed third parties and other PSPs.

While information types depicted significant differences in the baseline scenario, acceptability did not differ significantly anymore, for most information flows, once transmission principles were added. This demonstrates that recipient and principles might be more important than information types. This was observed among all three payment solutions. The direction of increase or decrease of acceptability is consistent for all transmission principles and all payment solutions, which indicates two points: Firstly, respondents' answers are logically sound and consistent, which helps strengthen the validity of the study. Secondly, digital euro transactions may not be seen as completely different compared to the existing payment methods, as has bene also observed in existing research (Tronnier et al., 2023). However, acceptability of information flows is notably lower for the digital euro group among most baseline scenarios and among most scenarios involving transmission principles. These results are also consistent between information types. A possible explanation could be user familiarity and market penetration of existing payment solution. This was also speculated for IoT devices in prior work (Apthorpe et al., 2018). The comparison of PayPal and Online Banking transactions also reveals that acceptability in the baseline scenario is overall higher for Online Banking transactions, and no clear trend can be observed when adding transmission principles. Apthorpe et al. (2018) argue that privacy norms can be identified through particularly low or high acceptability scores among groups and information flows. For instance, the government, other PSPs and third parties, are generally seen as inappropriate recipients of data in the baseline scenario and retain notably lower AAS than the central and house bank even when transmission principles are added. On the other hand, little difference between information-type is observed,

which remains constant among most information flows. We therefore argue that privacy norms likely depend on the recipient and transmission principle rather than the information type. Moreover, privacy norms may not generally differ between CBDC transactions and existing digital payment solutions. Prior work that utilized identical transmission principles (e.g., use of data for advertising) demonstrated similar results in the smart home context (Apthorpe et al., 2018).

6. Limitations and Future Work

The limitations of this work relate to the topic itself, as well as to the applied methodology and approach in this study. CBDC are still in its infancy with only a limited number of them being deployed, with data on usage and technology being not readily available. We therefore focused on the digital euro as one specific CBDC that is transparency communicated upon by the ECB to European citizens. Respondents were nonetheless not able to use the digital euro, and their understanding of the concept of CBDC might be limited. However, research suggests that attitudes towards an unknown technology, or payment solution, are formed through attitudes towards existing solutions (Tronnier et al., 2023). We aimed to mitigate this issue by surveying understandability of respondents and using introductory information provided by the ECB. The results of this work may not directly be transferable to other countries, citizens and CBDC, as this study was performed with solely German-speaking individuals to control for the differences in CBDC design and cultural factors. Defining privacy norms is not an easy task and often relies on assumptions and simplifications (Harborth & Pape, 2021). Actual information flows could therefore differ from the possibilities surveyed in this work in terms of recipients and data transferred. This leaves room for future work to study the transfer of specific data types or to study different CBDC within different countries. This includes CBDC that are designed to act as a store of value, as well as privacy concerns related to cross-border use of interoperable CBDC.

This study is therefore to be seen as a first step towards a comprehensive analysis of privacy norms in both CBDC and existing digital payment solutions.

7. Conclusion and Contributions

This work is the first to study the acceptability of flows of information in digital payment transactions, in particular for CBDC, in detail. Using a quantitative approach, we surveyed 1064 respondents to gather acceptability scores for a wide variety of contextual integrity parameter combinations, to provide a first step towards the identification of privacy norms in CBDC payments. Under contextual integrity theory, information flows that are deemed inappropriate by users violate privacy norms (Nissenbaum, 2009) thereby resulting in privacy concerns. As such concerns are found to hinder CBDC adoption intention (Tronnier et al., 2022), identifying appropriate information flows and privacy norms is vital for the successful development of CBDC.

The results indicate that acceptability of information flows, depends in particular on the recipient of information rather than on information type, answering *RQ1*. Different transmission principles are consistently able to increase or decrease perceived appropriateness of information flows across recipients and information types. The results further indicate that the appropriateness of information flows differs only to a limited degree between digital euro and PayPal or Online Banking transactions, answering *RQ2*. While both exhibit somewhat higher levels of appropriateness, this might be due to familiarity and market penetration of the existing payment solutions.

As a theoretical contribution, this work is the first to apply contextual integrity theory towards CBDC and to evaluate information flows across digital payment methods. We find that privacy norms are likely to be similar between existing and future payment solutions and are violated if unacceptable data recipients, e.g., third parties, the government, or specific transmission principles, e.g., data used to improve recipients' services, are involved.

As a practical contribution, CBDC developers and central banks may use the developed CI framework for CBDC and the results of this work to create CBDC that confirms with end-user privacy norms. This includes the clear and transparent communication of data transmission principles and possible recipients. For instance, the prevention of illegal activities was found to even increase acceptability of information flows.

Acknowledgement
This work was co-funded through the EU-funded CybserSecPro Project [Agreement no. 101083594].

References

Allen, S., Čapkun, S., Zhang, F., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., & Wüst, K. (2020). Design Choices for Central Bank Digital Currency: Policy and Technical Considerations.

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering Smart Home

Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*.

Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review*.

Auer, R., Böhme, R., Clark, J., & Demirag, D. (2023). Mapping the Privacy Landscape for Central Bank Digital Currencies. *Communications of the ACM*.

Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., & Shin, H. S. (2022). Central bank digital currencies: motives, economic implications, and the research frontier. *Annual review of economics*, *14*, 697-721.

Bandara, R., Fernando, M., & Akter, S. (2020). Privacy concerns in E-commerce: A taxonomy and a future research agenda. *Electronic Markets*, *30*(3).

Baronchelli, A., Halaburda, H., & Teytelboym, A. (2022). Central bank digital currencies risk becoming a digital Leviathan. *Nature Human Behaviour*.

Bech, M., & Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review*

Bitkom. (2023). *Nutzen Sie Online-Banking?* https://de.statista.com/statistik/daten/studie/476716/umfrage/umfrage-zur-online-banking-nutzung-in-deutschland/

Chaum, D., Grothoff, C., & Moser, T. (2021). *How to issue a central bank digital currency; How to issue a central bank digital currency*.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Erlbaum Associates.

Coppola, D. (2023). *Share of online stores that offer the main payment methods in Germany in 2020*.

Dionysopoulos, L., Marra, M., & Urquhart, A. (2023). Central Bank Digital Currencies: A Critical Review. *Available at SSRN 4354985*.

Dogan, A., & Bicakci, K. (2023). KAIME : Central Bank Digital Currency with Realistic and Modular Privacy. *Cryptology EPrint Archive*.

Eurogroup. (2022). *Digital euro Privacy options*.

European Central Bank. (2020). *Report on a digital euro*. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

European Central Bank. (2021). *Eurosystem report on the public consultation on a digital euro* (Issue April). https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

European Central Bank. (2022). *Progress on the investigation phase of a digital euro*.

Fang, W., Liu, N., Pan, Q., & Zhou, B. (2023). The trilateral game of privacy perception, financial regulation and central bank digital currency issuance. *Journal of Accounting, Business and Finance Research*, *16*(2), 44–52.

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. *SSRN Electronic Journal*.

Hamm, P. (2022). Acceptance Factors for Cryptocurrencies as Payment Systems. *Proceedings of the 55th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2022.729

Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality Apps – A vignette based online experiment. *Computers in Human Behavior*, *122*, 106833.

Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). Mobile Payments: Consumer Benefits & New Privacy Concerns. *SSRN Electronic Journal*.

Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance*, *64*.

Kosse, A., & Mattei, I. (2023). *Making headway - Results of the 2022 BIS survey on central bank digital currencies and crypto*. www.bis.org

Lagarde, C., & Panetta, F. (2021). *Key objectives of the digital euro*. https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html

Lee, Y., Son, B., Park, S., Lee, J., & Jang, H. (2021). A survey on security and privacy in blockchain-based central bank digital currencies. *Journal of Internet Services and Information Security*, *11*(3), 16–29.

Nissenbaum, H. (2009). *Privacy in context*. Stanford University Press.

Reith, R., Buck, C., Walther, D., Lis, B., & Eymann, T. (2020). How privacy affects the acceptance of mobile payment solutions. *27th European Conference on Information Systems (ECIS)*.

Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., Khatib, S. F. A., & Amosh, H. Al. (2022). The Research Trend of Security and Privacy in Digital Payment. *Informatics*, *9*(2).

Schueffel, P. (2023). CBDCs: Pros and Cons - A Comprehensive List and Discussion of the Advantages and Disadvantages of Central Bank Digital Currency. *SSRN Electronic Journal*.

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. F. (2018). Analyzing Privacy Policies Using Contextual Integrity Annotations. *SSRN Electronic Journal*, 1–18.

Smith, H. J., Dinev, T., & Xu, H. (2011). *Information Privacy Research: An Interdisciplinary Review*.

Solberg Söilen, K., & Benhayoun, L. (2022). Household acceptance of central bank digital currency: the role of institutional trust. *International Journal of Bank Marketing*, *40*(1), 172–196.

Tronnier, F., & Biker, P. (2022). A Framework and Qualitative Evaluation of Privacy Concerns in the Digital Euro. *PACIS 2022 Proceedings*.

Tronnier, F., Harborth, D., & Biker, P. (2023). Applying the extended attitude formation theory to central bank digital currencies. *Electronic Markets*, *33*(1).

Tronnier, F., Harborth, D., & Hamm, P. (2022). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, *53*, 101158.

Wadsworth, A. (2018). The pros and cons of issuing a central bank digital currency. *Reserve Bank of New Zealand Bulletin*, *81*(7), 1–21.