https://doi.org/10.33271/nvngu/2026-4/211

V. Koziuk,
orcid.org/0000-0002-5715-2983,
Yu. Ivashuk,
orcid.org/0000-0002-8459-4744,
N. Tsyapa*,
orcid.org/0009-0005-0820-5443

West Ukrainian National University, Ternopil, Ukraine
* Corresponding author e-mail: 7syapa@gmail.com

DOES PRIVACY PARADOX SURVIVE WHEN CONTEXT MATTERS?

Purpose. To assess whether the privacy paradox persists when accounting for contextual information and transparency in digital services, and to evaluate the stability of privacy preferences across everyday life, social media, and digital finance.

Methodology. A questionnaire survey of 400 respondents was conducted. Indices of privacy propensity in three domains and indices of preference for privacy over convenience and over undefined future benefits were constructed on Likert scales and analyzed using descriptive statistics, correlation analysis, t-tests, and regression models.

Findings. Privacy propensities differ significantly across contexts and correlate only weakly with each other. At the same time, all three indices of propensity for privacy are strongly and statistically significantly related to the preference for privacy over functionality when the choice is formulated in a clear, context-rich way, which supports the conclusion that the privacy paradox in this setting appears in a weak form and that context acts as a boundary line between the privacy paradox and more preference-consistent choices. That said, the explanatory power of the models remains modest and does not justify a strong rational-choice interpretation.

Originality. The study jointly examines three context-distant privacy domains and explicitly contrasts abstract and contextualized privacy-functionality trade-offs, showing that context acts as a boundary condition between the privacy paradox and rational, preference-consistent choice. In contrast to the authors' previous work on the privacy paradox in Central Bank Digital Currencies (CBDC) design and trust in them, this article extends the analysis to three non-CBDC domains of everyday life. This includes social media, and digital finance, and explicitly contrasts abstract and context-rich privacy-functionality trade-offs within a single empirical design.

Practical value. The results suggest that clearer and more context-rich privacy choices are associated with greater preference consistency, which highlights the potential value of more transparent privacy policies and user interfaces in digital services. For regulators, the findings provide only preliminary support for transparency-oriented approaches to privacy policy, as the cross-sectional design and non-probabilistic sample do not allow strong causal or normative conclusions.

Keywords: *digital economy, digital privacy, privacy paradox, behavioral economy, consumer choice*

Received: 02 March 2026
Accepted: 16 July 2026
Available online: 27 August 2026

Introduction. Digitalization is changing usual connections in society and forms of social interactions. What was previously the norm now looks like an inefficient allocation of time and effort due to availability of digital services and social networks. Digital services significantly minimize search costs, transform transaction costs, and form new modalities of consumer behavior. Payment habits and methods of maintaining interactions among economic agents, financial intermediaries, and regulators undergo similar changes. However, the broader the opportunities become in the digital world, the more it demands our personal data. Personal data have long turned into a resource for building better algorithms. And competition between companies relying on data-driven business models increasingly concerns the issue of how much personal data allow algorithms to be better tuned [1]. The development of artificial intelligence is likely to accelerate this trend by adding competition between an individual's actual data and simulated data based on real people's data, which further increases the value of personal data.

Can privacy be exchanged for the better ability of digital services to satisfy client needs? The issue of privacy's role in behavior within the digital environment is actively debated [2, 3]. A persistent gap between stated privacy concerns and actual online behavior has attracted considerable scholarly attention [4, 5]. Nevertheless, research results do not indicate an obvious consensus regarding the key issue of how much economic agents value privacy in principle and the extent to which the stated privacy preference is confirmed in actual actions [6, 7]. The difference between stated and revealed preferences has been termed the "privacy paradox". At the same time, the existence of substantial arguments suggesting that the "privacy paradox" is a consequence of the design of empirical tests rather than a behavioral distortion [8] can have far-reaching consequences for how digital services will be developed and regulated.

Given the importance of the "privacy paradox" problem and critical approaches to this phenomenon from the perspective of the context that affect behavior [9], this article empirically tests choice alternatives between the privacy and functionality of digital services (privacy functionality trade-off). From previous studies it is known that the propensity for general privacy, privacy in the digital environment, and privacy in the financial environment may differ, and the relative transi-

© Koziuk V., Ivashuk Yu., Tsyapa N., 2026

tivity of the corresponding preferences may indicate the presence of a "privacy paradox" in a soft form [10].

Does this mean there are grounds to doubt that individuals with a higher level of stated propensity for privacy will demonstrate a consistent preference for greater protection of their data rather than the functional efficiency of digital services, which depends on access to their data? Based on a survey of 400 respondents, it is established that a direct but weak relationship is observed among the propensity for everyday privacy, the propensity for privacy in social networks, and the propensity for privacy in digital finance, while the latter is the least correlated with the previous two. Furthermore, personal respondent data such as age, gender, income level, or digital service skills have weak explanatory power when it comes to specific dimensions of privacy. The choice between the alternatives of privacy and digital service functionality (privacy functionality trade-off) is sensitive to the extent to which respondents correlate such a choice with a specific context. In a more abstract formulation of the choice alternative, the transitivity of preferences decreases, whereas in a more specific contextual formulation of the choice alternative, the transitivity of preferences becomes statistically significant. This indicates that the phenomenon known as the "privacy paradox" may contain a strong component of behavioral distortion regarding the perception of context in an environment with information asymmetry. Such results are consistent with the view that information transparency may be a relevant consideration for privacy protection policy, though the present study does not provide direct normative evidence for specific regulatory prescriptions.

Literature review. The issue of digital privacy has an important economic dimension. On the one hand, personal data serves as a raw material for tuning algorithms designed to better satisfy consumer needs, thereby improving companies' competitive positions. On the other hand, the personalization of consumer offers does not preclude price discrimination, which grants firms excessive economic power over consumers and reduces social welfare. This raises the question of what the policy on personal data protection should be.

Research on the privacy paradox problem has clearly divided into several directions.

The first direction encompasses works emphasizing that the privacy paradox accompanies economic behavior in the digital world. In early studies, scholars assert a significant difference between stated and actual privacy preferences, and this result has been replicated in more recent experiments. For example, individuals who claim they value their privacy are often willing to disclose personal data in exchange for relatively small benefits, and their stated concern does not correlate with actual disclosure behavior when using digital services [11, 12]. According to Cofone [13], such a difference is often perceived as an argument for a substantial behavioral distortion underlying the privacy paradox. Chhabra [14] identify four reasons why economic agents may behave in accordance with the privacy paradox. These reasons include privacy calculus as a method of rational behavior, information asymmetry as an example of bounded rationality, the bandwagon effect as a behavioral distortion, and trust as a manifestation of decision-making heuristics. Based on experimental tests, Chhabra [14] conclude that the privacy paradox is empirically confirmed, with information asymmetry and the peanut effect explaining it.

The second direction involves studies that develop the idea of the privacy paradox. A focus on age groups indicates the presence of a "new privacy paradox". The stereotypical perception that the generation more involved in using social networks and digital services cares less about privacy does not correspond with several empirical findings. As Hargittai and Marwick [15] demonstrate, the younger generation is well aware of the privacy problem in the digital environment and applies privacy protection measures. At the same time, the perception of an indifferent attitude towards privacy through the "no hide" approach may be mistaken due to a resigned attitude towards data that has already entered the digital environment. Therefore, if data is already digitized, the importance of privacy protection at subsequent stages loses its fundamental meaning. Digital privacy remains a persistent social norm, and younger generations are often more knowledgeable about how to protect their personal data than the older generation [16, 17]. Another example of behavior is a situation where economic agents consciously choose to neglect the privacy problem through privacy cynicism to rationalize their choice in an informationally complex environment [18].

The cross-cultural aspect of privacy also matters. Liyanaarachchi [19] states that the relationship between the propensity for privacy and beliefs regarding power distance is significantly determined by culture. Concurrently, Koziuk and Ivashuk [20] note that institutional factors may outweigh cultural factors in terms of their impact on the choice between privacy and functionality. Colnago [21] draw attention to another dimension of the privacy problem. In their experimental model, individuals who take privacy dismissively also act to ensure it, similarly to how individuals stating a strong privacy preference do not take corresponding actions. Colnago [21] named this phenomenon the reversed privacy paradox.

The third direction comprises studies arguing that the privacy paradox is more a consequence of experimental design than a denial of the economic agent's rational behavior. Solove [22] states that specific experimental conditions placing respondents in unnatural situations do not replicate behavior based on a clear understanding of the privacy problem, the value of personal data, and an awareness of the consequences of their dissemination. Cofone [13] emphasizes that the privacy paradox aligns more with a known behavioral distortion regarding the reaction to structural uncertainty and time discounting. Cofone [13] demonstrates that the modality of choice in the privacy context is not a typical economic exchange. A typical temporal problem in economics involves sacrificing a present benefit in favor of uncertain future benefits. Conversely, the choice regarding privacy relates more to opting for present benefits in exchange for uncertain future losses. Such an exchange structure contains several important components that may be mistakenly perceived as a prerequisite for the privacy paradox. The temporal aspect implies that economic agents are prone to higher discounts of more distant future benefits or losses. The structural un-

certainty aspect suggests that economic agents behave as if dealing with a case of asymmetric information. The contextual aspect influences whether this primarily concerns information asymmetry or future discounting.

The fourth direction encompasses works presenting attempts to rationalize the privacy paradox or at least explain why economic agents might exhibit inconsistency in preferences despite being rational [23]. One option for rationalizing the privacy paradox is the privacy calculus approach. Brits and Jonker [24] confirm this using the example of financial application usage. Furthermore, researchers draw attention to the importance of context. Context reduces the level of information asymmetry while simultaneously determining the extent to which economic agents share structural uncertainty with their counterparties [3, 4]. Context ultimately conditions the degree to which economic agents will demonstrate consistency in stating, manifesting, and confirming their preferences [9]. A series of empirical tests regarding the willingness to share personal data when using digital financial services revealed that the issue of trust, understanding the context of interactions, and the counterparty's profile significantly affect privacy behavior [25, 26]. Using the example of CBDCs, Koziuk [10] states that the propensity for privacy does not inherently prove the superiority of anonymity over functionality. Instead, trust in the institution expected to provide such anonymity correlates with trust in the institution's ability to actually ensure it. Therefore, it is evident that context significantly influences the reduction of structural uncertainty. Similarly, the complexity of the informational choice environment substantially impacts economic agents' ability to maintain consistent preferences [23, 13]. The domain-specific nature of privacy decisions further compounds this effect, as preferences formed in one context do not readily transfer to another [22]. Koziuk [27] demonstrates that combining structurally dissimilar choice options can lead preferences to merge into complexly organized patterns, making the privacy paradox a matter of interpretational bias.

This article empirically confirms that the propensity for everyday privacy, privacy in social networks, and privacy in digital finance may correlate weakly with each other due to the distance between their contexts. However, these propensities correspond statistically significantly with a choice in favor of privacy rather than the functionality of digital services in cases where the context allows a better connection between potential benefits and practical everyday experience. Conversely, a loss of preference consistency becomes obvious when the context of the alternative regarding the privacy or functionality of digital services is more blurred. These findings contribute to the discussion that context significantly weakens the assumption of the privacy paradox's dominance while simultaneously confirming that this issue is relevant to personal data protection regulatory policy. Transparency designed to lower the informational barrier to understanding choices appears, based on the reviewed literature, to be associated with a higher likelihood that choices will align with stated privacy preferences.

Based on the reviewed literature on the privacy paradox, context effects, and information asymmetry in digital environments, the following hypotheses are formulated:

H1. Privacy propensity indices across three domains – everyday life, social media, and digital finance – differ significantly in their distributions, reflecting domain-specific framing effects rather than a single, uniform privacy disposition.

H2. Privacy propensity indices across domains correlate only weakly with each other, indicating limited preference transitivity when contexts differ.

H3. Privacy propensity indices are more strongly associated with preferences for privacy over functionality when the choice is formulated in a context-rich and concrete way (IPPUFB) than when it is formulated in abstract terms (IPPC).

H4. Personal demographic characteristics (gender, age, education, income, and digital literacy) explain only a limited share of the variance in privacy propensity indices and privacy-functionality trade-offs, which is consistent with a context-driven rather than a purely trait-driven view of privacy behavior.

Methods. The research methodology is based on the empirical processing of respondent data. For the purposes of this study 400 respondents were surveyed remotely by distributing a questionnaire via Google forms. Incomplete surveys were not considered. The survey was conducted online using a self-administered questionnaire distributed via Google Forms through academic and professional networks. In total, 400 fully completed questionnaires were retained for analysis. Due to the open distribution mode, the total number of individuals who received or accessed the survey link was not recorded, and a precise response rate cannot be calculated. The final sample consists of 240 women (60.0 %) and 160 men (40.0 %). The majority of respondents are 18–24 years old (62.3 %), with additional groups aged 25–34 (16.2 %), 35–44 (12.0 %), 45–54 (8.2 %), 55–64 (1.0 %), and 65+ (0.2 %). Regarding education, 23.8 % report secondary education, 15.5 % incomplete higher or college education, 27.0 % a bachelor's degree, 20.5 % a master's degree, and 13.2 % a doctoral degree (PhD or Doctor of Science). In terms of income, 31.0 % indicate monthly resources exceeding 20,000 UAH, 28.2 % prefer not to report or find it difficult to answer, while the remaining respondents are distributed across lower income brackets. Self-assessed digital literacy is predominantly medium (51.2 %) or high (40.0 %), with only 8.8 % reporting a low level, and almost all respondents use the Internet daily (97.8 %). Table 1 summarizes the main demographic characteristics of the sample.

The empirical design relies on identifying the connection between variables reflecting personal characteristics of the respondents, their propensity for privacy, and variables reflecting their preferences regarding the willingness to exchange a portion of data sharing for certain benefits from using digital services.

Personal characteristics are determined by gender, age, education level, computer literacy level, and income level. For empirical analysis gender is transformed into a binary variable; the age proxy is determined as the middle of the interval; computer literacy level is quantified based on a 3-point scale, the income level on a 7-point scale, and the education level on a 5-point scale. The Shapiro-Wilk test formally rejects normality for all five indices ($p < 0.001$); however, skewness and kurtosis coefficients remain close to zero for the majority of dis-

Table 1

Sample characteristics ($N = 400$)

Characteristic	Category	*N*	%
Gender	Female	240	60.0
	Male	160	40.0
Age	18–24 years	249	62.3
	25–34 years	65	16.2
	35–44 years	48	12.0
	45–54 years	33	8.2
	55–64 years	4	1.0
	65+ years	1	0.2
Education level	Secondary education	95	23.8
	Incomplete higher/college	62	15.5
	Higher (bachelor's)	108	27.0
	Higher (master's)	82	20.5
	Doctoral degree (PhD/Doctor of Science)	53	13.2
Monthly income (UAH)	Less than 3,000	37	9.2
	3,000–6,000	40	10.0
	6,000–10,000	33	8.2
	10,000–15,000	26	6.5
	15,000–20,000	27	6.8
	More than 20,000	124	31.0
	Difficult to say/Prefer not to answer	113	28.2
Digital literacy level	Low – uses only basic functions	35	8.8
	Medium – confidently uses basic digital services	205	51.2
	High – well oriented in digital tools and settings	160	40.0
Internet use frequency	Daily	391	97.8
	Several times a week	6	1.5
	Once a week	3	0.8

tributions, indicating that the departure from normality reflects the discrete nature of the Likert-based scores rather than substantive asymmetry. Given the sample size of $N = 400$, the Central Limit Theorem provides sufficient justification for the application of parametric procedures – paired-samples t-tests, Pearson correlation, and OLS regression – which are robust to moderate violations of normality at this sample size.

Propensities for privacy are determined based on responses to 4 questions across 3 domains and are quantified on a 5-point Likert scale. A similar approach was substantiated and applied in Koziuk [10, 27]. However, in this article 4 questions were chosen that are more focused and context-oriented, due to which the obtained results regarding the evaluation of the propensity for privacy are methodologically different from previous studies. Regarding everyday privacy the questions are as follows. "Do you prefer to meet with friends at your home?". "Do you believe that disclosing information about wealth improves the operation of digital services?". "Are you ready to share personal hygiene items?". "Do you often talk about the circumstances of your life during a long journey?". The everyday privacy propensity index (PEP) is intentionally designed to capture a broad, trait-like propensity for privacy in everyday life rather than a narrow measure of digital privacy concerns. This operationalization follows the multidimensional view of privacy in the literature, where privacy is not limited to informational control but also encompasses physical, social, and psychological dimensions. Empirical research demonstrates that social privacy concerns describe individuals being afraid of their social relationships being negatively affected when others get access to personal information, while physical privacy concerns are associated with negative physical consequences that may arise when information about individuals' habits and physical whereabouts is misused [28]. Accordingly, items such as willingness to share personal hygiene objects or to disclose personal circumstances during a long journey are treated as indicators of physical and social boundary management, which complement items more directly related to informational privacy. This interpretation is further supported by research conceptualizing the need for privacy as a cross-situational tendency to actively and consciously define, communicate and pursue a desired level of privacy, distinguishing four components – informational, social, psychological, and physical – and noting that this need manifests across various everyday life situations [29]. In this study, PEP is therefore interpreted as a general privacy propensity construct capturing cross-situational boundary maintenance, while PSMP and PDFP capture domain-specific privacy propensities in social media and digital finance respectively. Regarding the propensity for privacy in social media the questions sound like this. "Do you think it is better when a social media profile is open?". "Do you share information in social media about personal experiences and moments of your personal life such as travels, visiting interesting events and places, or meeting friends?". "Do you try to fill out your social media profile as completely as possible and make changes to it on time?". "Is the fact that your personal data is used for commercial purposes without your knowledge acceptable to you even when it improves the services you may consume?". Regarding the propensity for privacy in digital finance the questions are the following. "Do you prefer digital and remote forms of monetary transactions even if they require initial customer identification?". "Is the fact that the traceability of financial transactions may become a norm in society acceptable to you?". "Are you indifferent to the fact that the forms of carrying out a transaction such as cash, card payment, or cryptocurrency payment differ for reasons of the ability to guarantee your anonymity?". "Do you agree with the opinion that full anonymity and non-traceability of money transactions is not the best choice for society?".

The results of the answers based on the Likert scale are summed up, thanks to which 3 indicators are obtained. These are the propensity for everyday privacy (PEP), the propensity for social media privacy (PSMP), and the propensity for digital finance privacy (PDFP). Subsequently, a descriptive statistic of the obtained three indices and the connections between them are provided. The more similarly these values are distributed and the stronger the correlation between them, the more the transitivity of preferences is confirmed. That is if a respondent is more prone to privacy in everyday life, they should also demonstrate a higher propensity for privacy when using social media and digital finance. If there are significant differences between the distribution of values

of these indices and the correlation is weak, such a result can be qualified as a privacy paradox. However, in this case the design of the questions allows that context may influence the transitivity between the three propensities. To check the impact of personal characteristics on privacy propensities regression analysis is applied.

To assess the internal consistency of the three privacy propensity indices, Cronbach's α was computed for each subscale using the raw survey data. The everyday privacy propensity index (PEP) achieved an α of 0.43, the social media privacy propensity index (PSMP) an α of 0.52, and the digital finance privacy propensity index (PDFP) an α of 0.32. These values indicate modest internal consistency, particularly in the case of PDFP, and are therefore interpreted as evidence that the indices capture only loosely correlated but theoretically related aspects of privacy propensity rather than highly homogeneous latent traits. The indices are thus used as exploratory composite measures, and their limitations are explicitly acknowledged in the interpretation of results.

At the same time, the present study relies on internal consistency measures rather than full confirmatory factor analysis (CFA). Given the modest Cronbach's α values, particularly for PDFP, future research should complement this exploratory approach with CFA to examine convergent and discriminant validity of the PEP, PSMP, and PDFP subscales in line with best practices in privacy scale development [30].

In the next stage the index of preference for privacy over convenience (IPPC) and the index of preference for privacy over undefined future benefits (IPPUFB) are constructed. The first index is designed to evaluate how ready respondents are to share their personal data to obtain more functional digital services. Instead, the second is more context-oriented with a focus on practical cases of using digital services, meaning it is less abstract. The indices are built based on the summation of responses to 5 questions quantified on a 5-point Likert scale.

In the first case the questions are as follows: "For me, service convenience is more important than guarantees of the confidentiality of my data"; "I am ready to give up some app functions if it allows for better protection of my data"; "Speed of access to the service is more of a priority for me than time spent on configuring privacy settings"; "I choose products that are less convenient but better known for strong data protection"; "The possibility of getting a quick result justifies the transfer of additional personal data".

In the second case the questions are as follows: "I am ready to provide my search history to receive more accurate and relevant results"; "I will allow tracking of my purchases if it allows providing me with exclusive discounts unavailable to others"; "I will agree to the collection of data about my location if a taxi service finds me much faster"; "I will allow the analysis of my financial transactions if it allows receiving a personalized financial plan from the bank"; "I am ready to provide more personal data during registration if it allows receiving instant decisions, for example, approval of applications".

The obtained quantitative values of the preference for privacy over convenience (IPPC) and the preference for privacy over undefined future benefits (IPPUFB) as dependent variables are analyzed for similarity of distribution and density of the correlation connection. A weak connection and dissimilarity of distribution will indicate a privacy paradox. Subsequently the obtained indices are regressed with personal characteristics and quantitative values of PEP, PSMP, and PDFP as independent variables. In the case of a direct and dense connection between IPPC and IPPUFB on the one hand and PEP, PSMP, and PDFP on the other, the transitivity of preferences will dominate over the privacy paradox. Otherwise, the lack of consistency between privacy propensities and preferences for privacy over functionality or future benefits will indicate a privacy paradox. It should also be considered that the nature of the relationship between IPPC and PEP, PSMP, and PDFP and between IPPUFB and PEP, PSMP, and PDFP may differ due to conditional structural uncertainty, since the preference for privacy over functionality has a more abstract expression than clear probable benefits from less cautious privacy in clear contextual cases.

Table 2 provides a summary of descriptive statistics for all five constructed indices prior to the main analysis.

Results of empirical analysis. ***Propensity for privacy in three different contexts.*** The main idea of identifying the propensity for privacy based on questions directly related to social experience relies on the assumption that this variable can better reflect the baseline position of the respondent's preferences than stating a privacy preference revealed in response to a direct question during a survey [10]. The analysis of the propensity for privacy across three scenario-realistic but unrelated contexts allows us to see how consistent respondents are.

The statistical characteristics of the distribution of quantitative values of the propensity for privacy across the three contexts allow us to see obvious differences in preferences. Thus, the mean value of the propensity for everyday privacy (PEP) was 13.31, the propensity for so-

Table 2

Descriptive statistics of the five constructed indices ($N = 400$)

	PEP	PSMP	PDFP	IPPC	IPPUFB
N	400	400	400	400	400
Median	13.00	14.00	11.00	16.00	18.00
Mean (arithmetic)	13.31	13.79	10.97	16.57	18.01
Std. Deviation	2.464	2.711	2.271	2.956	4.064
Skewness	–0.090	–0.126	0.449	0.480	–0.053
Std. Error of Skewness	0.122	0.122	0.122	0.122	0.122
Kurtosis	–0.002	–0.490	0.384	1.762	–0.516
Std. Error of Kurtosis	0.243	0.243	0.243	0.243	0.243
Shapiro-Wilk	0.983	0.982	0.970	0.932	0.972
P-value of Shapiro-Wilk	<0.001	<0.001	<0.001	0.001	<0.001
Minimum	6.000	6.000	6.000	7.000	7.000
Maximum	20.00	20.00	20.00	25.00	25.00

Note. PEP = everyday privacy propensity; PSMP = social media privacy propensity; PDFP = digital finance privacy propensity; IPPC = index of preference for privacy over convenience; IPPUFB = index of preference for privacy over undefined future benefits. Cronbach's α: PEP = 0.43, PSMP = 0.52, PDFP = 0.32 (computed on raw item data).

cial media privacy (PSMP) was 13.79, and the propensity for digital finance privacy (PDFP) was 10.97. The median values are respectively 13, 14, and 11. And the mode values are 14, 12, and 10. The standard deviation is 2.46, 2.71, and 2.27. More obvious differences are visible from the comparison of the box plots (Fig. 1). The data presented in Fig. 1 indicate that the distributions of the corresponding indices deviate from normality. The Shapiro-Wilk test confirms this for all three indices: PEP $W = 0.983$, $p < 0.001$; PSMP $W = 0.982$, $p < 0.001$; PDFP $W = 0.970$, $p < 0.001$. The distributions of PEP and PSMP are both approximately symmetric, with Skewness coefficients of –0.090 and –0.126, respectively (SE = 0.122), neither of which is statistically significant ($|z| < 1.96$). PDFP is the only index with statistically significant positive asymmetry: Skewness = +0.449 ($z = 3.68$, $p < 0.001$), indicating that the majority of respondents cluster toward lower values of digital finance privacy propensity with a tail extending toward higher scores.

The obtained values of $p < 0.01$ allow us to reject the null hypothesis regarding the normal distribution of all three indices.

The application of the *t*-test also confirms that the mean values of the PEP, PSMP, and PDFP indices have statistically significant differences. In all cases of pairwise comparisons including PEP vs PSMP, PEP vs PDFP, and PSMP vs PDFP the null hypothesis about the statistical similarity of the means is rejected. If in the first case $p < 0.001$ is observed, then in the next two $p < 0.000$ as seen in Table 1. Differences in the nature of the distribution affected the correlation between the indices. In all cases of pairwise correlations a low value of the corresponding coefficient and weak statistical significance are observed according to Table 3. Similar results occur in the case of simple regression analysis presented in Table 3.

The obtained data clearly indicate that the consistency of preferences in different contexts is violated. It can be said that the contours of context are a natural barrier to the transitivity of preferences. On the one hand, this is evidence of the privacy paradox. On the other hand, a greater focus on context in the questionnaire structure requires a more careful interpretation of the data obtained. First, this applies to PDFP. As can be seen from Fig. 1 and Table 3, the propensity for privacy in digital finance is the most distant and at the same time the least pronounced. This is somewhat paradoxical considering that the index of propensity for privacy in social media has the highest mean and median value and the strongest right-skewed distribution of the three, while the index of propensity for privacy in social media has the highest mean and median values of the three, while the index of propensity for privacy in digital finance has the lowest mean, median, and mode values and the only statistically significant positive skew among the three indices. Considering the content of the questions based on which PDFP is calculated, it can be assumed that respondents do not show stronger reservations about financial privacy due to payment experience formed within the fulfillment of KYC and AML requirements by financial intermediaries. This assumption was confirmed in the regression analysis.

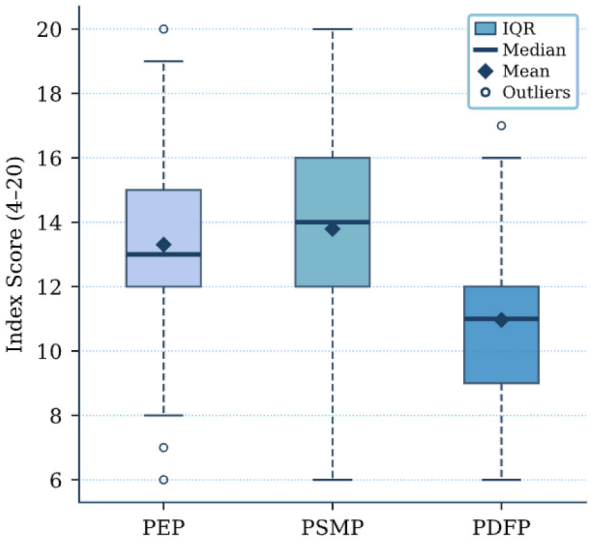

Fig. 1. Distribution of the privacy propensity indices across three domains

Note. Box = IQR (25^{th}–75^{th} percentile); whiskers = 1.5 × IQR; ◆ = mean; $n = 400$

Table 3

Statistical characteristics of relationships between privacy propensity indices in three contexts

	PEP vs PSMP	PEP vs PDFP	PSMP vs PDFP
t-test	–3.2163 $p < 0.0014$	14.5460 $p < 0.0000$	16.4627 $p < 0.0000$
Correlation coefficient	0.33*	0.08	0.06
Coefficient *b* of the linear approximation function and R^2	0.364 0.11	0.074 0.007	0.053 0.004

* *Note*. indicates statistical significance at the level of $p < 0.05$.

In a first approximation it can be argued that the transitivity of preferences regarding the propensity for privacy is violated by the framework of context. The experience of respondents may play a role in shaping what requires more privacy and what does not. The boundaries of privacy as a social stereotype can be flexible. Such boundaries can be different in different contexts.

Influence of personal characteristics on privacy propensity indices. It is known from previous studies that personal characteristics can play a significant role in determining attitudes toward privacy. It is traditionally believed that men are less open, and age is positively related to privacy preferences [31]. The results obtained to some extent fall in line with established ideas, but at the same time have several nuances. The indices of propensity for privacy PEP, PSMP, and PDFP were chosen as dependent variables. The independent variables are gender, age, education level from primary to academic degree of Doctor of Philosophy and above, digital literacy level, and income level. Independent variables except for the age variable are determined based on the Likert scale. The results of the regression analysis are shown in Table 4.

As can be seen from Table 4, the statistical properties of the obtained regression dependencies except for the PSMP case are low. That is personal characteristics as a whole are not reliable explanatory variables. At the same time gender has a statistically significant positive corre-

Table 4

Results of regression analysis of the impact of personal characteristics on the propensity for privacy across three contexts

	PEP	PSMP	PDFP
Gender	0.005 (0.20) $p = 0.84$	**1.02** (3.69) $p = 0.0001$	0.019 (0.076) $p = 0.94$
Age	**0.06** (3.61) $p = 0.000$	**0.056** (3.0) $p = 0.003$	0.02 (1.24) $p = 0.22$
Education level	0.15 (1.2) $p = 0.23$	0.21 (1.55) $p = 0.12$	–0.12 (–1.03) $p = 0.3$
Digital literacy level	0.06 (0.29) $p = 0.78$	0.13 (0.58) $p = 0.56$	–0.21 (–1.085) $p = 0.28$
Income	–0.087 (–1.44) $p = 0.15$	–0.08 (–1.26) $p = 0.2$	**–0.14** (–2.38) $p = 0.02$
F statistics	$F(5,394) = 6.3387$	$F(5,394) = 9.7514$	$F(5,394) = 2.7004$
R^2	0.07	0.11	0.03

* *Note*. Bold indicates a statistically significant coefficient value. Values in parentheses represent t-statistics

lation with the propensity for privacy exclusively in the case of social media, meaning men are less open than women. In the case of PEP and PDFP the gender variable although having a theoretically expected sign is statistically insignificant. Age is in a statistically significant relationship exclusively in the case of the propensity for everyday privacy and the propensity for privacy in social media. The level of education and the level of digital literacy are not in a statistically significant relationship with the corresponding indices, and in the case of PDFP the corresponding variables have a negative sign. The latter can be interpreted as an example of the fact that education provides better awareness of the functioning of digital finance and the restrictions on the anonymity of transactions arising from the current regulatory environment. This thesis is confirmed by a statistically significant inverse relationship between the level of income and PDFP, which, as already mentioned, is somewhat paradoxical at first glance. Income also has an inverse relationship in the first two equations, but with insufficient statistical significance. It can be assumed that income is a specific proxy for confidence that weakens the propensity for privacy.

In general, the low statistical quality of all three models indicates that personal characteristics do not play a decisive role in shaping the propensity for privacy in the analyzed contexts.

Transitivity of preferences regarding privacy and functionality in different information setups. Testing the impact of behavioral factors on the transitivity of preferences is an important element of the analysis [13]. To take behavioral nuances into account the structure of the questionnaire made it possible to distinguish between responses with more abstract and more specific formulations. Accordingly, the index of preference for privacy over convenience (IPPC) and the index of preference for privacy over undefined future benefits (IPPUFB) were obtained. The difference between them lies in a more abstract attestation of preferences in the first case and a focus on context in the form of choice alternatives from realistic situations in the second. Since context is recognized as an important factor in behavior and attitudes toward privacy [9], the difference in formulations will reflect the probable difference in choosing among alternative situations. Also, this test will allow identifying behavioral nuances that are important for revealing privacy preferences [13]. For example, more abstract formulations may cause less understanding or expose the individual to perceiving the situation as reflecting a higher level of uncertainty. Instead, more specific questions related to a choice that can be correlated with real experience will have a greater impact on the perception of the situation in the temporal dimension.

That is the identity of the statistical parameters of IPPC and IPPUFB will indicate the transitivity of preferences and the absence of behavioral distortions caused by the influence of uncertainty and information perception. In other words, an abstract choice among alternatives will be equivalent to a choice among more contextual alternatives. The results obtained regarding the statistical properties of IPPC and IPPUFB are not unambiguous. On the one hand, there is an obvious and statistically significant correlation between both indices. The correlation coefficient is 0.58 at $p < 0.05$. For example, this is a much stronger correlation compared to the one between the privacy propensity indices. On the other hand, the statistical properties of IPPC and IPPUFB are quite different. The null hypothesis regarding the similarity of the means can be rejected with high statistical significance: $t(399) = -8.343$, $p < 0.001$ (paired-samples t-test), confirming that respondents systematically score higher on IPPUFB ($M = 18.01$, SD = 4.064) than on IPPC ($M = 16.57$, SD = 2.956). The Shapiro-Wilk test rejects normality for both indices (IPPC: $W = 0.932$, $p < 0.001$; IPPUFB: $W = 0.972$, $p < 0.001$); however, skewness coefficients remain modest (IPPC: +0.480; IPPUFB: –0.053), and given $N = 400$, parametric inference is appropriate. Fig. 2 presents box plots comparing the distributions of IPPC and IPPUFB, il-

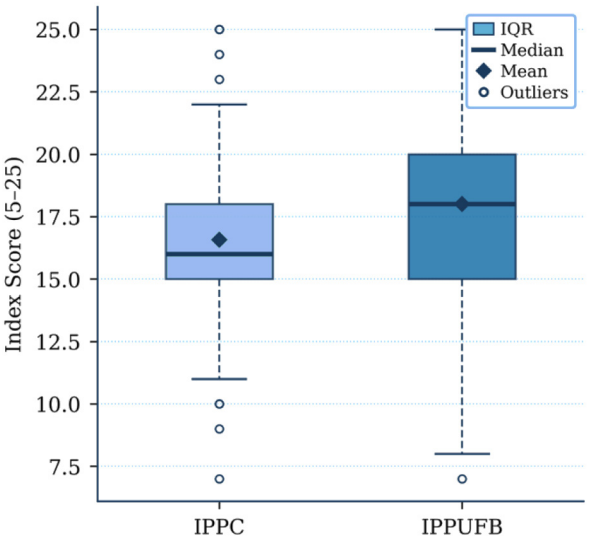

Fig. 2. Box plots of IPPC and IPPUFB distributions

Note. Box = IQR (25^{th}–75^{th} percentile); whiskers = 1.5 × IQR; ◆ = mean; $n = 400$

lustrating differences in central tendency, spread, and skewness between the two indices.

As can be seen from Fig. 2, the corresponding indices have significant differences in the distribution profile. IPPUFB has a much more pronounced right-skewed distribution and is more variable. For example, the standard deviation of IPPC is 2.956, while for IPPUFB it is 4.064.

The obtained results allow us to state that the transitivity of preferences in narrower contexts is more stable, but it is sensitive to behavioral reactions to a particular information setup.

The impact of the propensity for privacy on the choice between the privacy and functionality of digital services. In the next stage the influence of personal characteristics and the propensity for privacy across the three contexts on preferences regarding the use of digital services was tested. The index of preference for privacy over convenience (IPPC) and the index of preference for privacy over undefined future benefits (IPPUFB) were chosen as dependent variables.

The results of the regression analysis are shown in Table 5.

As can be seen from the data in Table 5, there is a significant difference in the statistical quality of the model with IPPC and with IPPUFB. The R^2 values of 0.08 for IPPC and 0.17 for IPPUFB indicate that the models explain only a small share of the variance in preferences for privacy over functionality or undefined future benefits. These results should therefore be interpreted as evidence of statistically significant but modest associations rather than as fully predictive models of privacy-related choice behavior. In particular, the findings do not warrant any strong claims that individuals' choices are rational in a strict economic sense; instead, they suggest that privacy propensities have a limited but detectable influence on privacy-functionality trade-offs when the context is clearly articulated. In first approximation this is the evidence that the behavioral factor can significantly influence preferences depending on the information setup. In conditions of a more clearly articulated context

Table 5

Results of regression analysis of the impact of personal characteristics and propensity for privacy on the choice between the privacy and functionality of digital services

	IPPC	IPPUFB
Gender	**–0.79** (–2.14) $p = 0.03$	–0.09 (–0.095) $p = 0.92$
Age	0.02 (0.98) $p = 0.33$	0.06 (1.76) $p = 0.079$
Education level	–0.16 (–0.88) $p = 0.37$	–0.32 (–1.32) $p = 0.19$
Digital literacy level	**0.59** (1.98) $p = 0.04$	0.35 (0.88) $p = 0.38$
Income	0.08 (0.94) $p = 0.34$	0.12 (1.01) $p = 0.31$
PEP	0.096 (1.18) $p = 0.2$	**0.3** (3.02) $p = 0.002$
PSMP	**0.23** (3.34) $p = 0.000$	**0.43** (4.68) $p = 0.000$
PDFP	**0.16** (2.13) $p = 0.03$	**0.39** (3.85) $p = 0.000$
F statistics	$F(8,391) = 4.2374$	$F(8,391) = 10.226$
R^2	0.08	0.17

* *Note.* Bold indicates a statistically significant coefficient value. Values in parentheses represent t-statistics

the relationship between the choice in favor of higher privacy and the explanatory factors is much more stable.

A more detailed look reveals that privacy propensity indices and the choice in favor of the alternative privacy versus functionality are in a dense and statistically significant relationship in a situation of a more clearly articulated context. In the case of a more abstract formulation of the choice alternative a direct relationship is also traced, but its statistical significance takes place only in the case of PSMP and PDFP with a slightly lower value of the coefficients. Regarding personal characteristics they do not play a statistically convincing role in the case of IPPUFB, and in the case of IPPC only gender and the level of digital literacy have a statistically significant relationship. At the same time the gender variable demonstrates a negative sign in both cases, meaning women are more willing to disclose their personal data. Age rather encourages more cautious handling of self-disclosure. The same applies to the level of digital literacy and the level of income. In contrast, the level of education inversely affects the level of readiness to disclose personal data when using digital services.

Taken together, the empirical results show that when respondents better understand the context in which a choice between privacy and the benefits of data sharing is made, their behavior aligns more closely with the transitivity of preferences. At the same time, the information setup determines the extent to which behavioral

distortions deviate actual choices regarding privacy from underlying privacy propensities.

Discussion. The obtained results allow for a better understanding of the limitations of the privacy paradox approach and strengthen the focus on the problem of information transparency as a prerequisite for the correspondence between preferences and choice. Context can therefore significantly influence the stability of preference ordering, and what is often described as a privacy paradox may partly mimic context-driven differences in the way preferences are elicited rather than a fundamental inconsistency in preferences themselves. At the same time there are significant differences compared to the earlier study by Koziuk [10]. For example, a more defined context when determining the propensity for privacy weakens the transitivity of preferences. Moreover, if the privacy paradox is interpreted in terms of the coincidence of preferences in different contexts, its existence should be acknowledged as it takes place, for example, in Koziuk [32]. But if the privacy paradox is interpreted in terms of the loss of consistency of preferences within contextual boundaries, the obtained results rather do not confirm it according to the principle of how it is demonstrated by Kokolakis [23] and Cofone [13].

The obtained results correlate with a broader view that the privacy paradox is strongly shaped by contextual factors that influence the relationship between privacy attitudes and behavior [23]. They also align with systematic empirical evidence that discrepancies between expressed privacy concerns and actual online behavior vary depending on how specific contexts of data disclosure are framed [3, 4]. In addition, studies show that both the particular domain of data use and concrete application settings, such as financial apps, crucially determine whether a privacy paradox or a more calculative, context-sensitive pattern of disclosure is observed [24, 9]. The focus of Cofone [13], on contrasting structural uncertainty and discounting the future does not contradict the results obtained in this article. Respondents better correlate their choice regarding privacy and their own propensity for it where the level of uncertainty decreases. The alternative between accessing data now in exchange for undefined benefits in the future, being context-driven, does not affect the loss of transitivity of preferences.

A more precise theoretical account of this mechanism can be offered by combining Cofone's framework of structural uncertainty [13] with Nissenbaum's concept of contextual integrity [33]. Nissenbaum argues that individuals do not evaluate information disclosure in abstract terms but rather assess whether a given flow of personal data conforms to the norms governing a specific social context – norms of appropriateness and distribution that are already internalized through lived experience. Under this view, the IPPUFB items, which frame each data-sharing choice within a recognizable everyday scenario (a taxi service, a bank, a loyalty program), allow respondents to invoke such pre-existing contextual norms, thereby reducing the structural uncertainty that Cofone identifies as the proximate cause of inconsistent behavior. The IPPC items, by contrast, present the privacy-functionality trade-off in terms that lack an identifiable contextual anchor, leaving respondents to navigate the choice under full structural uncertainty, which manifests empirically as lower preference consistency and weaker alignment with stated privacy propensities. The observed gap between IPPC and IPPUFB coefficients in Table 5 is therefore interpretable not merely as a measurement artefact but as evidence that contextual integrity – the activation of domain-specific informational norms, operates as the micro-level mechanism through which reduced structural uncertainty translates into more preference-consistent choices.

The question of the normative consequences of the obtained results remains debatable. On the one hand, the fact of the privacy paradox is often cited as a reason for the lack of privacy regulation in the digital environment [22]. On the other hand, Cofone [13] emphasizes the more significant problem of information asymmetry as a result of which economic agents may behave inconsistently. From our study it follows that the nature of the information setup can have an impact on behavioral distortions in the transitivity of preferences regarding privacy, but if economic agents better understand the context, their preferences correlate more strongly with the propensity for privacy. This suggests that transparency may be an important facilitating condition for greater alignment between privacy preferences and actual choices, though the causal direction and generalizability of this association remain open questions for future research.

A clear distinction must be drawn between the present article and the authors' earlier work on the privacy paradox in the context of central bank digital currencies (CBDCs). While the CBDC-oriented studies by Koziuk, Ivashuk, and Hayda [10] and Koziuk, et al. [27, 32] focus on privacy preferences, trust in central banks, and anonymity-functionality trade-offs in CBDC design, using data from multi-country samples and CBDC-specific choice scenarios, the current article examines privacy behavior in three context-distant but CBDC-neutral domains: everyday life, social media, and digital finance. The present survey employs a distinct questionnaire, a different sample, and an alternative empirical design that contrasts abstract versus context-rich privacy-functionality trade-offs (IPPC vs. IPPUFB) for generic digital services rather than CBDCs. Methodologically, the earlier papers also explore AI-based interpretation and association-rule mining in the CBDC setting, whereas the current study relies on classical regression analysis to link three privacy propensity indices to two types of privacy-functionality choices across multiple domains. The contribution of this article is therefore incremental in two respects: it generalizes the privacy paradox discussion beyond CBDC design to a broader digital services environment, and it demonstrates that context-rich formulations strengthen the alignment between privacy propensities and privacy-favoring choices even when trust in a specific monetary institution is not part of the decision frame.

Limitations. The sample was obtained via a non-probabilistic, convenience sampling strategy using an online questionnaire distributed through academic and professional networks. Consequently, the absolute number of individuals who received or accessed the survey link was not recorded, and a precise response rate cannot be established. The sample is relatively young (with more than 60 % of respondents aged 18–24) and highly digitally engaged (almost 98 % re-

port daily Internet use and over 90 % medium or high digital literacy), which implies that the findings cannot be straightforwardly generalized to the broader population. The direction of this selection bias is not straightforward, however, and its implications differ across indices. Younger, digitally engaged respondents are likely to be more aware of privacy risks and more familiar with contextualized data-sharing scenarios, which may overestimate the strength of the association between IPPUFB and the privacy propensity indices relative to what would be observed in a more age-representative sample. At the same time, this cohort may exhibit greater tolerance for data disclosure in exchange for functional benefits due to habitual use of social media and digital services – a pattern consistent with the online apathy and sense of powerlessness over shared data documented by Hargittai and Marwick [15], which could conversely attenuate the observed IPPC values. The net effect is therefore ambiguous: the sample composition may simultaneously inflate context-sensitivity effects and compress the abstract preference-for-privacy scores, making it difficult to determine whether the gap between IPPC and IPPUFB would narrow or widen in an age-balanced sample. Future research should replicate the results using probability-based sampling strategies, a broader age structure, and a wider geographic coverage.

From a modelling perspective, the relatively low R^2 values of 0.03–0.17 indicate that both personal characteristics and privacy propensities account for only a limited share of the variance in privacy-related choices. This suggests that additional factors such as trust, past digital experience, perceived risk, and specific design features of digital services, which were not observed in the present study, are likely to play an important role. Existing evidence from related contexts supports this expectation: for example, Koziuk [10] shows that trust in the issuing institution explains a sizeable share of variation in preferences over anonymity versus functionality in CBDC design, over and above baseline privacy propensities. By analogy, one would expect that augmenting the present models with measures of institutional trust, perceived risk of data misuse, and past experience with data breaches could raise R^2 beyond the 0.03–0.17 range observed here, while leaving the qualitative pattern – namely the stronger alignment between contextualized privacy-functionality trade-offs (IPPUFB) and privacy propensities compared to abstract trade-offs (IPPC) – intact. As a result, the empirical analysis should be regarded as exploratory, and the conclusions are deliberately constrained to describing statistically significant associations rather than providing a full structural explanation of privacy-functionality trade-offs.

Conclusion. The privacy paradox continues to remain an important framework for analyzing behavior in the digital environment. Empirical tests demonstrate that the privacy preference is often not confirmed in actual actions due to behavioral distortions or information asymmetry. The context of the choice regarding the disclosure of personal data is considered a powerful factor explaining the privacy paradox. This influenced the analytical structure of this study. Considering the probability of differences between stated and confirmed privacy preferences as well as the vulnerability of choice consistency to the nature of the information setup, the logic of empirical testing of respondents' preferences regarding the use of digital products was built. The survey data used made it possible to calculate indices of propensity for everyday privacy, propensity for privacy when using social media, and propensity for privacy in digital finance, as well as indices of preference for privacy over convenience and the index of preference for privacy over undefined future benefits. Based on the obtained data it is confirmed that context significantly determines the consistency of preferences. Thus, a weak correlation is observed between the three indices of propensity for privacy, while a correlation is observed between the indices of preference for privacy in different information setups. At the same time the three indices of propensity for privacy and the two indices of choice in favor of privacy in different information setups demonstrate different distribution parameters and statistically significant differences in the means. Theoretically, this may indicate a weak form of the privacy paradox. However, regression analysis demonstrated that privacy propensity indices well explain the choice in favor of privacy when using digital products, but under conditions of a more informationally transparent choice architecture. Differences in the density of the connection depending on the information setup confirm that the privacy paradox often mimics the problem of choice in conditions of a lack of transparency.

The results of the empirical test allow us to assert that context and information setup have an impact on the consistency of preferences. The clearer the context, the stronger the correlation between the propensity for privacy and the choice in favor of privacy, while a substantial share of the variance in privacy-related choices remains unexplained. Personal demographic characteristics such as gender, age, education, income, and digital literacy – explain only a limited share of the variance in both privacy propensity indices and privacy-functionality trade-offs. With the exception of gender and age in selected models, demographic variables do not demonstrate statistically significant explanatory power, which reinforces the conclusion that privacy behavior is driven more by contextual framing than by individual traits. This pattern is consistent with the idea that clearer information setups help individuals make more preference-consistent decisions, but it does not allow us to conclude that behavior is fully rational in a strict economic sense. The privacy paradox may reflect the problem of mixing contexts within which economic agents can demonstrate different choice patterns. Transparency plays a significant role in the ability of economic agents to behave consistently. These findings suggest that clearer contextual framing is associated with greater preference consistency in privacy-related choices. To the extent that this association reflects a genuine mechanism, it points to the potential relevance of context-sensitive privacy notice design and layered consent architectures for digital service providers. For regulators, the results offer exploratory support for transparency-oriented approaches, but given the cross-sectional design and modest explanatory power of the models, causal and prescriptive conclusions are not warranted at this stage.

References.

1. Hu, Q., Xie, J., & Zhang, G. (2023). The role of data-driven services strategy in platform competition: A system performance perspective. *PLoS ONE, 18*(1), e0272547. https://doi.org/10.1371/journal.pone.0272547

2. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442-492. https://doi.org/10.1257/jel.54.2.442

3. Goldfarb, A., & Que, V. F. (2023). The economics of digital privacy. *Annual Review of Economics, 15*(1), 267-286. https://doi.org/10.1146/annurev-economics-082322-014346

4. Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

5. Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226-261. https://doi.org/10.1016/j.cose.2018.04.002

6.Gimpel, H., Kleindienst, D., & Waldmann, D. (2018). The disclosure of private data: Measuring the privacy paradox in digital services. *Electronic Markets, 28*(4), 475-490. https://doi.org/10.1007/s12525-018-0303-8

7. Cloos, J., Frank, B., Kampenhuber, L., Karam, S., Luong, N., Moller, D., Monge-Larrain, M., ..., & Rossler, C. (2019). Is your privacy for sale? An experiment on the willingness to reveal sensitive information. *Games, 10*(3), 28. https://doi.org/10.3390/g10030028

8. Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics, 41*, 55-69. https://doi.org/10.1016/j.tele.2019.03.003

9. Hirschprung, R. S. (2023). Is the privacy paradox a domain-specific phenomenon? *Computers, 12*(8), 156. https://doi.org/10.3390/computers12080156

10. Koziuk, V., Ivashuk, Y., & Hayda, Y. (2024). CBDC, trust in the central bank, and the privacy paradox. *Economics – Innovative and Economics Research Journal, 12*(2), 219-242. https://doi.org/10.2478/eoik-2024-0025

11. Athey, S., Catalini, C., & Tucker, C. E. (2017). The digital privacy paradox: Small money, small costs, small talk. *NBER Working Paper, 23488*. https://doi.org/10.3386/w23488

12. Chen, L., Huang, Y., Ouyang, S., & Xiong, W. (2021). The data privacy paradox and digital demand. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3930095

13. Cofone, I. (2026). The privacy paradox is a misnomer: Data under structural uncertainty. *Georgetown Law and Technology Review, 10*(1), 1. https://doi.org/10.2139/ssrn.6030275

14. Chhabra, S., Mukherjee, J., & Agarwal, M. N. (2023). Understanding privacy paradox: Experimental approach on study privacy concerns and actual behavior among apps users. *Journal of Organizational Computing and Electronic Commerce, 33*(3-4), 105-124. https://doi.org/10.1080/10919392.2023.2251328

15. Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737-3757. https://ijoc.org/index.php/ijoc/article/view/4655

16. Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2479938

17. Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology, 56*(1), 8-29. https://doi.org/10.1111/cars.12227

18. Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), 7. https://doi.org/10.5817/CP2016-4-7

19. Liyanaarachchi, G. (2021). Managing privacy paradox through national culture: Reshaping online retailing strategy. *Journal of Retailing and Consumer Services, 60*, 102500. https://doi.org/10.1016/j.jretconser.2021.102500

20. Koziuk, V., & Ivashuk, Y. (2022). Does it matter for CBDC design? Privacy-anonymity preferences from the side of hierarchies and egalitarian cultural patterns. *Economics – Innovative and Economics Research Journal, 10*(1), 35-53. https://doi.org/10.2478/eoik-2022-0008

21. Colnago, J., Cranor, L. F., & Acquisti, A. (2023). Is there a reverse privacy paradox? An exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. *Proceedings on Privacy Enhancing Technologies, 2023*(1), 455-476. https://doi.org/10.56553/popets-2023-0027

22. Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review, 89*(1), 1-51. https://doi.org/10.2139/ssrn.3536265

23. Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. https://doi.org/10.1016/j.cose.2015.12.001

24. Brits, H., & Jonker, N. (2023). The use of financial apps: Privacy paradox or privacy calculus? *De Nederlandsche Bank Working Paper, 794*. https://www.dnb.nl/media/hwpei2bx/working_paper_no-794.pdf

25. Cruijsen, C. van der (2020). Payments data: Do consumers want banks to keep them in a safe or turn them into gold? *Applied Economics, 52*(6), 609-622. https://doi.org/10.1080/00036846.2019.1659493

26. Rosati, P., Fox, G., Cummins, M., & Lynn, T. (2022). Perceived risk as a determinant of propensity to adopt account information services under the EU Payment Services Directive. *Journal of Theoretical and Applied Electronic Commerce Research, 17*(2), 493-506. https://doi.org/10.3390/jtaer17020026

27. Koziuk, V., Dziubanovska, N., & Tsegelnyy, I. (2025a). Can artificial intelligence help to identify privacy paradox: Case of CBDC. *CEUR Workshop Proceedings, 3974*, 119-132. https://ceur-ws.org/Vol-3974/paper13.pdf

28. Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal, 32*(6), 1126-1157. https://doi.org/10.1111/isj.12386

29. Frener, R., Dombrowski, J., & Trepte, S. (2023). Development and validation of the Need for Privacy Scale (NFP-S). *Communication Methods and Measures, 17*(4), 265-290. https://doi.org/10.1080/19312458.2023.2246014

30. MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293-334. https://doi.org/10.2307/23044045

31. Choi, S., Kim, B., Kim, Y.-S., & Kwon, O. (2023). Central bank digital currency and privacy: A randomized survey experiment. *BIS Working Paper, 1147*. https://www.bis.org/publ/work1147.htm

32. Koziuk, V., Ivashuk, Y., & Hayda, Y. (2025b). Privacy preferences and trust in central banks: Heterogeneity in case of CBDC. *Financial and Credit Activity: Problems of Theory and Practice, 3*(62), 11-26. https://doi.org/10.55643/fcaptp.3.62.2025.4734

33. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119-157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

Чи існує парадокс приватності? Роль контексту

*В. В. Козюк, Ю. П. Івашук, Н. Г. Цяпа**

Західноукраїнський національний університет, м. Тернопіль, Україна

* Автор-кореспондент e-mail: 7syapa@gmail.com

Мета. Дослідження має на меті з'ясувати чи зберігається парадокс приватності з урахуванням контекстної інформації та прозорості цифрових сервісів, а також перевірити стійкість преференцій щодо приватності в повсякденному житті, соціальних медіа й цифрових фінансах.

Методика. Проведено анкетне опитування 400 респондентів. На основі результатів були визначені індекси схильності до приватності у трьох доменах й індекси переваги приватності над зручністю та над невизначеними майбутніми вигодами. Були використані методи шкали Лікерта, аналізу за допомогою описової статистики, кореляційного аналізу, t-тестів і регресійних моделей.

Результати. Схильності до приватності суттєво відрізняються залежно від контексту й лише слабо

корелюють між собою. Водночас, усі три індекси перебувають у тісному та статистично значущому зв'язку із перевагою приватності над функціональністю за умови чіткого контекстного формулювання вибору, що підтверджує висновок про існування парадоксу приватності у слабкій формі. Також це свідчить про те, що контекст є розмежувальною лінією між парадоксом приватності й більш преференційно узгодженим вибором. Зрештою, пояснювальна сила моделей залишається скромною й не дає підстав для сильної інтерпретації в дусі раціонального вибору.

Наукова новизна. У дослідженні одночасно розглядаються три контекстно віддалені домени приватності та явно зіставляються абстрактні й контекстуалізовані компроміси «приватність–функціональність», що демонструє роль контексту як граничної умови між парадоксом приватності й раціональним, преференційно узгодженим вибором. На відміну від попередніх робіт авторів, присвячених парадоксу приватності в контексті цифрових валют центральних банків (ЦВЦБ) і довіри до них, ця робота поширює аналіз далі за контекст ЦВЦБ. Це включає такі домени як повсякденне життя, соціальні медіа й цифрові фінанси, і явно зіставляє абстрактні та контекстно насичені компроміси «приватність–функціональність» у єдиному емпіричному дизайні.

Практична значимість. Результати показують, що коли вибір щодо приватності подано чіткіше й у зрозумілому контексті, споживачі частіше роблять вибір, який краще відповідає їхнім заявленим уподобанням. Це вказує на можливу користь прозоріших політик приватності та зрозуміліших рішень в оформленні цифрових сервісів. Для регуляторів ці результати радше свідчать на користь підходів, заснованих на прозорості, однак через перехресний характер дослідження й невипадкову вибірку вони не дають підстав для сильних причинних чи нормативних висновків.

Ключові слова: *цифрова економіка, цифрова приватність, парадокс приватності, поведінкова економіка, споживчий вибір*