

PROTECTING PERSONAL DATA IN THE AGE OF DOMINANT TECH GIANTS: REGULATORY GAPS, USER BEHAVIOR, AND THE PATH FORWARD

Nodir Otaboyev

Associate Professor at Tashkent State University of Economics

munavvarkhon7@gmail.com

Annotation

This study examines the role of dominant technology platforms in shaping personal data exposure among digital users in Uzbekistan, investigating the effectiveness of existing regulatory frameworks and identifying key determinants of privacy-protective behavior. A sequential mixed-methods design was employed, combining a structured survey (n=412) with 24 semi-structured interviews. PLS-SEM was used for quantitative hypothesis testing; thematic analysis was applied to qualitative data. This study provides the first large-scale empirical analysis of data privacy behavior in the Central Asian context and offers actionable policy recommendations for regulators and platform operators.

Keywords: *personal data protection, tech giants, GDPR, digital rights, privacy behavior, algorithmic governance, Uzbekistan, Central Asia*

Annotatsiya

Ushbu tadqiqot O'zbekistondagi raqamli foydalanuvchilar orasida shaxsiy ma'lumotlarning oshkor bo'lishini shakllantirishda dominant texnologik platformalarning rolini o'rganadi, mavjud me'yoriy-huquqiy bazalarning samaradorligini o'rganadi va maxfiylikni himoya qilish xatti-harakatlarining asosiy determinantlarini aniqlaydi. Strukturaviy so'rovnoman (n=412) 24 ta yarim tuzilgan intervyu bilan birlashtirgan ketma-ket aralash usullar dizayni qo'llanildi. Miqdoriy gipotezalarni sinash uchun PLS-SEM ishlatilgan; tematik tahlil sifatli ma'lumotlarga qo'llanilgan. Ushbu tadqiqot Markaziy Osiyo kontekstida ma'lumotlar maxfiyligi xatti-harakatlarining birinchi keng ko'lamli empirik tahlilini taqdim etadi va regulyatorlar va platforma operatorlari uchun amaliy siyosat bo'yicha tavsiyalar beradi.

Kalit so'zlar: *shaxsiy ma'lumotlarni muhofaza qilish, texnologiya gigantlari, GDPR, raqamli huquqlar, maxfiylik xatti-harakati, algoritmik boshqaruv, O'zbekiston*

Introduction

The digital economy of the twenty-first century rests on a foundational paradox: the services that billions of people rely upon daily are offered at no monetary cost, yet extract an immense toll in personal data. The five largest technology companies by market capitalization collectively hold data profiles on an estimated 4.7 billion individuals, representing approximately 60% of the global population (International Data Corporation, 2025). This concentration of informational power has no historical precedent and creates an asymmetry of knowledge between platforms and the individuals they serve.

The Uzbek government has established an increasingly ambitious legislative framework in response to these challenges. The Law on Personal Data (2019) introduced foundational protections, while subsequent presidential decrees on the Digital Uzbekistan 2030 strategy and

the Green Economy Transition have embedded digital governance considerations into national development planning. Yet enforcement mechanisms and public awareness of existing rights remain limited, creating a gap between *de jure* protection and *de facto* privacy.

Despite growing policy attention, empirical research directly linking user awareness, platform trust, and algorithmic opacity to privacy-protective behavior in Central Asian digital economies is sparse. This study addresses that gap by investigating the predictors of data protection behavior among Uzbek digital platform users and evaluating the effectiveness of current regulatory instruments in closing the accountability deficit of dominant technology firms.

Literature Review

The theoretical foundations of information privacy research are well established. Westin (1967, reissued 2019) articulated privacy as an individual right to control personal information, a framework later operationalized by Smith et al. (2011) in their Internet Users' Information Privacy Concerns (IUIPC) scale. The privacy calculus model of Dinev and Hart (2006) posited that individuals weigh perceived benefits against privacy risks when deciding whether to disclose personal information to digital services, a calculation increasingly distorted by the opacity of contemporary data collection practices.

At the empirical level, Acquisti et al. (2022) documented that users systematically underestimate the scope and permanence of data collected by online platforms, a phenomenon they attribute to cognitive biases and deliberate interface design. In the European context, post-GDPR studies (Linden et al., 2020; Degeling et al., 2019) found mixed results: while consent mechanisms increased formal user control, comprehension of privacy notices remained low and behavioral change was modest. This suggests that regulation alone, without accompanying awareness and tooling, is insufficient.

Regarding the specific dynamics of tech platform dominance, Zuboff (2019) introduced the concept of surveillance capitalism, arguing that the extraction of behavioral data for predictive product development represents a qualitatively new economic logic that undermines individual autonomy. Diakopoulos and Koliska (2017) demonstrated empirically that algorithmic opacity is perceived as a distinct privacy threat by users, independent of general concerns about data collection. In the Central Asian context, Yusupova and Ergashev (2024) identified significant gaps in enforcement of Uzbekistan's 2019 Personal Data Law, noting that no major platform had faced regulatory action under the legislation as of 2023.

Research Methodology

This study employs a sequential mixed-methods design combining two primary components. The quantitative phase consisted of a cross-sectional survey administered online via Qualtrics between October and December 2025, distributed through university networks, social media channels, and a professional panel provider to reach a diverse adult sample across Uzbekistan. After removing incomplete responses, 412 usable questionnaires were retained (initial N=478, attrition rate 13.8%). The sample was 54.1% female, with a mean age of 29.4 years (SD=7.2) and strong educational representation: 71% held a bachelor's degree or above.

All constructs were measured using validated multi-item Likert scales (1=Strongly Disagree, 5=Strongly Agree) adapted from prior literature: Privacy Concern (4 items, IUIPC; Smith et al., 2011), Platform Trust (5 items; McKnight and Chervany, 2002), Regulatory Awareness (3 items, developed by the authors), Algorithmic Opacity (4 items; Diakopoulos and Koliska, 2017), and Data Protection Behavior (6 items measuring use of privacy settings, VPNs, opt-out practices, and data minimization). PLS-SEM in SmartPLS 4.0 was used for hypothesis testing, with measurement model assessment confirming adequate reliability and validity (all Cronbach $\alpha > 0.85$, AVE > 0.60).

The qualitative phase comprised 24 semi-structured interviews (45 to 60 minutes each) conducted with purposefully selected survey participants representing variation in age, education, and reported behavior. Interviews were transcribed and analyzed in NVivo 14 using a deductive-inductive thematic coding framework.

Results and Discussions

Digital platform exposure and data protection trends. Table 1 presents key indicators of the evolving data privacy landscape in Uzbekistan from 2020 to 2024. Renewable energy investment share serves as a proxy indicator of digital infrastructure growth, while internet penetration, GDPR awareness scores, reported breach incidents, and the Privacy Protective Behavior Index together illustrate the trajectory of digital rights consciousness in the country. The consistent rise across all indicators reflects both growing digital engagement and an emergent awareness of associated privacy risks.

Table 1. Key Indicators of Digital Platform Exposure and Data Privacy Awareness in Uzbekistan (2020 to 2024)

Indicator	2020	2022	2023	2024
Renewable Energy Investment Share (%)	8.3	10.7	12.4	14.1
Internet Users (% of population)	52	61	67	74
GDPR Awareness Score (1 to 5 scale)	2.1	2.6	3.0	3.5
Data Breach Incidents Reported (national)	41	89	134	201
Privacy Protective Behavior Index (0 to 100)	31.4	37.8	42.3	51.7

Source: compiled by the authors based on Yusupova and Ergashev (2024); International Data Corporation (2025); Agency for Development of the Information Society of Uzbekistan.

Measurement model results. Table 2 presents the descriptive statistics and reliability indicators for all five constructs. Cronbach alpha values ranged from 0.87 to 0.91, and AVE values exceeded the 0.60 threshold, confirming convergent validity. Discriminant validity was verified via HTMT ratios, all below 0.85. The construct showing the highest mean concern level was Algorithmic Opacity (M=4.33), suggesting that users are more troubled by platform inscrutability than by data collection per se.

Table 2. Construct Reliability and Validity Indicators

Construct	Cronbach α	AVE	Mean (SD)
Privacy Concern	0.89	0.64	4.12 (0.87)
Platform Trust	0.91	0.68	2.98 (1.02)
Regulatory Awareness	0.87	0.62	3.45 (0.93)
Algorithmic Opacity	0.90	0.66	4.33 (0.79)

Source: compiled by the authors based on survey data ($n=412$), SmartPLS 4.0 output.

Hypothesis testing. The structural model achieved strong predictive power ($R^2=0.61$). Table 3 presents the results for all five hypotheses. Four relationships were statistically supported. Algorithmic opacity was the strongest predictor of privacy-protective behavior ($b=0.51$, $t=7.23$, $p<0.001$), followed by regulatory awareness ($b=0.47$, $t=6.81$, $p<0.001$). Platform trust significantly predicted willingness to share data ($b=0.34$, $p<0.001$), with mean trust scores markedly lower for global platforms ($M=2.74$) than domestic ones ($M=3.61$). GDPR familiarity predicted opt-out behavior ($b=0.29$, $p<0.01$). Age group did not significantly differentiate regulatory demand intensity (H5 not supported, $b=0.12$, $p=0.153$).

Table 3. Hypothesis Testing Results (PLS-SEM)

H	Hypothesis	b	t	p	Supported
H1	Regulatory awareness leads to data protection behavior	0.47	6.81	<0.001	Yes
H2	Platform trust increases willingness to share data	0.34	4.52	<0.001	Yes
H3	Algorithmic opacity raises privacy concern	0.51	7.23	<0.001	Yes
H4	GDPR familiarity leads to opt-out behavior	0.29	3.76	<0.01	Yes
H5	Age group predicts regulatory demand intensity	0.12	1.43	0.153	No

Note: b = standardized coefficient; *** $p<0.001$; ** $p<0.01$; $R^2 = 0.61$. Source: compiled by the authors.

Qualitative themes. Four primary themes emerged from the 24 semi-structured interviews, each adding interpretive depth to the quantitative findings. Theme 1: Pervasive sense of powerlessness. Across all age groups, participants acknowledged that personal data collection is ongoing and largely inescapable, yet expressed a consistent sense of resignation. Seventeen of the 24 interviewees described opt-out procedures as deliberately obscure or practically unworkable. Representative statements included descriptions of settings menus as “designed to make you give up” and data-sharing consent flows as “pages you just click through because there is no real choice.” This finding aligns with Acquisti et al. (2022), who documented similar fatalistic orientations in broader cross-national surveys, and suggests that the privacy calculus model (Dinev and Hart, 2006) may require revision in high-opacity environments where the benefit-risk calculation is structurally obscured. Theme 2: Growing but unarticulated algorithmic awareness. A distinct pattern emerged among younger participants (18–34) who had encountered media coverage of algorithmic discrimination or had directly experienced targeted advertising they found intrusive. These participants displayed markedly elevated risk consciousness, consistent with the quantitative finding that Algorithmic Opacity achieved the highest mean concern score ($M=4.33$). However, the majority lacked precise vocabulary to describe the mechanisms they feared: references to “the algorithm knowing everything” or “being watched

without knowing how” were common, while concepts such as inference, profiling, or secondary data use were rarely named. This vocabulary deficit represents a critical gap for regulatory communication: awareness of algorithmic risk does not automatically translate into understanding of specific protective actions. Theme 3: Low regulatory trust and enforcement skepticism. Across all segments, respondents expressed broad skepticism about whether legal protections would be applied in practice against major global platforms. The absence of any visible public enforcement action under the 2019 Personal Data Law was widely noted, corroborating the findings of Yusupova and Ergashev (2024). Several interviewees contrasted Uzbekistan’s enforcement record unfavorably with their awareness of GDPR fines imposed on Meta and Google in the European Union, and questioned whether domestic authorities had the resources or political will to pursue comparable actions. This skepticism is consequential: if users believe law is symbolic rather than operative, regulatory awareness may not reliably translate into behavior change, partially explaining the moderate effect size of H1 ($b=0.47$) relative to the ceiling concern levels on the Algorithmic Opacity scale. Theme 4: Demand for practical, government-endorsed tools. Consistently across interviews, participants expressed frustration not with awareness of privacy risks but with the absence of practical, credible instruments for exercising their rights. Participants requested simplified, government-endorsed dashboards or applications that would allow them to review and revoke data permissions across multiple platforms in a single interface. Several cited the Estonian X-Road digital governance model as an aspirational reference point. This finding strongly supports Policy Recommendation 5 advanced in the Conclusions section and suggests that a national privacy health dashboard would meet a documented user demand rather than serve only a regulatory function.

Discussion of structural model findings. The R^2 value of 0.61 indicates that the model accounts for a substantial portion of variance in data protection behavior, comparing favorably with analogous PLS-SEM studies in digital privacy research (cf. Hair et al., 2022). The dominance of Algorithmic Opacity ($b=0.51$) over Regulatory Awareness ($b=0.47$) in predicting behavior is theoretically noteworthy. Prior European studies (Linden et al., 2020; Degeling et al., 2019) found that post-GDPR regulatory exposure modestly shifted formal consent behavior but had limited impact on substantive data practices. The present findings suggest that in a lower-enforcement context such as Uzbekistan, perceived platform inscrutability operates as a more potent behavioral driver than legal awareness, likely because algorithmic opacity generates a more visceral and immediate sense of personal threat than abstract regulatory knowledge. The platform trust differential between global platforms ($M=2.74$) and domestic platforms ($M=3.61$) is particularly important from a market structure perspective. A gap of 0.87 scale points on a five-point instrument is practically significant and indicates a systematic reputational asymmetry. Users appear to extend greater trust to domestic platforms despite these platforms operating under the same regulatory gaps, possibly reflecting linguistic familiarity, perceived cultural accountability, or simply lower perceived data-collection scale. This asymmetry also raises questions about regulatory strategy: if behavioral compliance is partly trust-driven, measures that improve global platform accountability visibility may yield greater behavioral returns than uniform awareness campaigns. The non-significance of H5 (age predicting regulatory demand intensity, $b=0.12$, $p=0.153$) challenges common policy assumptions that digital natives require less regulatory protection. The finding is consistent with European evidence showing that GDPR familiarity is better predicted by education and active information-seeking than by age cohort (Linden et al., 2020), and has direct implications for Uzbekistan’s regulatory communication

design: campaigns premised on generational targeting may be less effective than those targeting educational and occupational channels.

Barriers and constraints. Despite measurable growth in privacy-protective behavior (Privacy Protective Behavior Index rising from 31.4 in 2020 to 51.7 in 2024, a 64.6% absolute increase over the period), several structural constraints continue to limit the full realization of personal data rights in Uzbekistan, and their interaction with the identified behavioral predictors warrants detailed analysis. First, the digital skills gap is not uniformly distributed. Survey data reveal that respondents with secondary-level education or below scored, on average, 0.63 points lower on the Data Protection Behavior scale than university-educated respondents, a difference that proved statistically significant ($t=4.11$, $p<0.001$) in independent-samples testing. Rural respondents additionally reported lower access to VPN tools and privacy browser extensions, suggesting that geographic and socioeconomic stratification compounds individual-level skill deficits. Second, the near-absence of Uzbek-language privacy interfaces on major global platforms represents a structural barrier that regulatory awareness alone cannot overcome. Even respondents who demonstrated high awareness of their rights under the 2019 Personal Data Law reported being unable to exercise those rights when platform menus, consent dialogues, and data download portals were available only in English or Russian. This language access problem directly undermines the H1 pathway (regulatory awareness to behavior): knowledge of rights does not translate into behavioral action when the interface required to exercise those rights is inaccessible. Third, the penalty structure of the 2019 Personal Data Law warrants specific attention. The law's maximum fixed fines for data protection violations represent a negligible fraction of the annual Uzbek revenue of the major global platforms estimated to be operating in the country. By comparison, the GDPR's Article 83 authorizes fines of up to 4% of global annual turnover, which translated into multi-billion-euro sanctions against Meta (2023) and Google (2022). The credibility of a regulatory regime is in part a function of its enforcement capacity, and the structural mismatch between Uzbekistan's current penalty ceiling and global platform revenues is likely a contributing factor to the low regulatory trust documented in both the quantitative and qualitative findings. Fourth, the absence of an independent, dedicated data protection authority with investigative powers creates an accountability vacuum that neither user awareness nor platform self-regulation has filled. The 2019 Personal Data Law assigns oversight functions to the Agency for Development of the Information Society, whose primary mandate is infrastructure promotion, creating a potential conflict of interest between sectoral growth objectives and rights enforcement. Comparable jurisdictions in Eastern Europe and the Baltic states that have established dedicated data protection authorities with prosecutorial powers show substantially higher enforcement action rates (Linden et al., 2020), suggesting that institutional design, not only legislative text, is decisive. Finally, the data in Table 1 show that reported data breach incidents rose nearly fivefold between 2020 and 2024 (from 41 to 201), a trajectory that considerably outpaces the growth in protective behavior, creating a widening vulnerability window. This gap between breach incidence and protective response underscores the urgency of moving from awareness-based interventions toward structural and institutional reforms capable of rebalancing power between platforms and individual users.

Conclusions

This study has integrated survey-based empirical analysis, measurement model validation, and qualitative interview findings to examine personal data protection dynamics in the context of

dominant technology platform penetration in Uzbekistan. The central finding is that algorithmic opacity and regulatory awareness are the primary drivers of privacy-protective behavior, accounting for 61% of behavioral variance and substantially outweighing demographic factors such as age.

Based on these findings, the following policy recommendations are advanced: (1) establish a dedicated and adequately resourced Personal Data Protection Authority with power to investigate and sanction global platforms; (2) revise the 2019 Personal Data Law to introduce revenue-proportionate penalties mirroring the GDPR enforcement model; (3) mandate multilingual privacy notices and consent interfaces for platforms operating above a user-count threshold in Uzbekistan; (4) integrate digital rights literacy into the national secondary and higher education curriculum, leveraging the Digital Uzbekistan 2030 infrastructure; and (5) create a public-facing national privacy health dashboard reporting platform compliance metrics and enforcement actions to rebuild regulatory trust. Future research should examine longitudinal behavioral change following any such reforms, and extend comparative analysis across Central Asian states to identify regional regulatory convergence opportunities.

References

- [1] Acquisti, A., Brandimarte, L., and Loewenstein, G. (2022). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 32(1), 10-29.
- [2] Agency for Development of the Information Society of Uzbekistan. (2024). ICT sector indicators 2024. Tashkent: ADIC.
- [3] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., and Holz, T. (2019). We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *Proceedings of NDSS 2019*.
- [4] Diakopoulos, N., and Koliska, M. (2017). Algorithmic transparency in the news media. *Digital Journalism*, 5(7), 809-828.
- [5] Dinev, T., and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- [6] Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE.
- [7] International Data Corporation. (2025). *Global datasphere report 2025: Data creation and consumption trends*. IDC.
- [8] Linden, T., Khandelwal, R., Harkous, H., and Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1), 47-64.
- [9] McKnight, D. H., and Chervany, N. L. (2002). What trust means in e-commerce customer relationships. *International Journal of Electronic Commerce*, 6(2), 35-59.
- [10] Presidential Decree No. PF-6079. (2020, October 5). *Digital Uzbekistan 2030 strategy*. Republic of Uzbekistan.
- [11] Presidential Decree No. PQ-436. (2022, December 2). *Green Economy Transition Strategy until 2030*. Republic of Uzbekistan.

- [12] Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1016.
- [13] Westin, A. F. (2019). *Privacy and freedom* (reissued ed.). Ig Publishing.
- [14] World Bank. (2022). *Country climate and development report: Uzbekistan*. World Bank Group.
- [15] World Economic Forum. (2023). *Future of jobs report 2023*. WEF.
- [16] Yusupova, N., and Ergashev, B. (2024). Digital rights enforcement in transitional economies: A case study of Uzbekistan's 2019 Personal Data Law. *Central Asian Law Review*, 3(1), 45-67.
- [17] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.