International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 01 Jan-Feb; 2026 Page. No. 1135-1146

To cite this article: Le Duy Hai (2026). FROM CONSENT TO CONTROL, RETHINKING PERSONAL DATA PROTECTION AND USER AGENCY IN SMARTPHONE-CENTRIC DIGITAL ECOSYSTEMS IN VIETNAM, International Journal of Research in Commerce and Management Studies (IJRCMS) 8 (1): 1135-1146 Article No. 662 Sub Id 1134

FROM CONSENT TO CONTROL, RETHINKING PERSONAL DATA PROTECTION AND USER AGENCY IN SMARTPHONE-CENTRIC DIGITAL ECOSYSTEMS IN VIETNAM

Le Duy Hai

Faculty of Economic Information System and Electronic commerce, Thuongmai University

DOI: https://doi.org/10.38193/IJRCMS.2026.8191

ABSTRACT

Vietnam's digital economy is increasingly smartphone-first: everyday activities such as messaging, payments, shopping, transportation, and public services are mediated by mobile applications and platform ecosystems. At the same time, personal data processing has intensified through app permissions, device sensors, background data flows, and cross-service profiling. Most contemporary privacy regimes rely on user consent as the primary legal and ethical basis for processing. In smartphone-centric ecosystems, however, consent is frequently reduced to rapid acceptance of permission prompts and privacy notices that users rarely read, understand, or can meaningfully negotiate. This paper develops a conceptual and contextual argument that consent-based data protection is structurally insufficient in smartphone environments, not because users are irrational, but because mobile ecosystems embed asymmetries of power, opacity of information flows, and design patterns that convert consent into an illusion of control. Using Vietnam as the focal context and drawing on interdisciplinary insights from information systems, digital governance, and privacy theory (including contextual integrity and user agency), the paper proposes a shift from consent to control: a governance logic emphasizing ongoing user manageability, system-level safeguards, and platform accountability. The paper synthesizes literature on mobile permissions and consent fatigue, analyzes key regulatory developments in Vietnam (with particular attention to Decree 13/2023/ND-CP), and outlines a control-oriented framework that links ecosystem design, governance instruments, and user capabilities. The contributions are threefold: (1) reframing personal data protection in smartphone-centric settings as a control problem rather than a consent problem; (2) articulating a Vietnam-specific contextual agenda that highlights enforcement and ecosystem dominance issues typical of emerging economies; and (3) offering actionable policy and design implications for regulators, operating system providers, and app/platform operators.

KEYWORDS: personal data protection; smartphone ecosystems; user consent; user control; mobile permissions; digital governance; contextual integrity; Vietnam

1. INTRODUCTION

Smartphones have become the primary interface between individuals and the digital economy. In Vietnam, the smartphone is not merely a communication device; it is an infrastructure for participation in platform-mediated services such as social networking, digital payments, e-commerce, ride-hailing, food delivery, and public e-services. This smartphone-first trajectory is consistent with broader regional patterns in Southeast Asia, where mobile access often precedes or substitutes for fixed broadband adoption. As a consequence, personal data protection has become an urgent governance challenge because data generation and processing are deeply embedded in daily routines and occur continuously through sensors (location, microphone, camera), behavioral traces (clickstreams, purchase histories), and inferred attributes (interests, creditworthiness, risk scores).

Regulatory responses around the world have frequently treated consent as the central mechanism through which individuals exercise autonomy over personal information. Consent is appealing because it aligns with liberal principles of choice and individual control, and it provides a clear compliance pathway for organizations: obtain consent, then process data. However, the operationalization of consent in smartphone environments is mediated by user interfaces, permission architectures, and platform ecosystems that users neither design nor control. In practice, users face repeated prompts, bundled privacy policies, and default settings that encourage acceptance. In Vietnam, as in many emerging smartphone economies, the dominance of a small number of operating systems and the widespread reliance on platform-based services amplify the practical limitations of consent.

This paper argues that the core problem is not simply that users fail to read privacy notices; rather, consent is structurally misaligned with smartphone-centric ecosystems. Smartphones concentrate power in operating system providers, app stores, and platform operators that can shape user choices through design and policy. Data flows are often invisible (e.g., background collection, third-party SDKs), making informed choice infeasible. Consequently, consent becomes an administrative ritual that transfers responsibility to individuals while organizations retain effective control. To address this mismatch, the paper proposes a shift from consent to control—a governance logic that emphasizes ongoing manageability of data access and use, system-level safeguards, and accountability mechanisms that reduce the burden on users.

Vietnam is selected as a focal context for three reasons. First, Vietnam has experienced rapid platformization with high smartphone uptake and intensive usage of messaging and financial apps. Second, Vietnam has introduced notable regulatory instruments for personal data protection, including Decree 13/2023/ND-CP (effective 1 July 2023), which clarifies consent requirements and organizational responsibilities. Third, Vietnam illustrates a broader class of emerging economies where enforcement capacity, public awareness, and platform dominance interact to shape privacy outcomes.

The paper addresses three research questions:
RQ1: Why do consent-based personal data protection mechanisms fail to deliver meaningful protection in smartphone-centric ecosystems?

RQ2: What does a control-oriented approach to personal data protection entail at the level of ecosystem governance (OS, platforms, apps) and user agency?

RQ3: How do Vietnam’s regulatory and market conditions shape both the limitations of consent and the feasibility of control-oriented governance?

The remainder of this paper is structured as follows. Section 2 reviews the literature on consent, mobile privacy, and user agency, and develops the conceptual foundations for a shift to control. Section 3 elaborates the Vietnam context, including key regulatory developments and smartphone-centric market features. Section 4 describes the methodological approach and analytic strategy. Section 5 presents the analysis, synthesizing mechanisms through which consent fails and articulating structural asymmetries in smartphone ecosystems. Section 6 introduces a control-oriented conceptual framework and discusses its implications. Section 7 outlines theoretical, policy, and design implications, and Section 8 concludes with limitations and future research.

2. Literature Review and Conceptual Foundations

2.1 Consent as a Dominant Governance Logic

Consent is widely treated as a cornerstone of personal data protection, embedded in major regulatory regimes and organizational compliance practices. In principle, consent operationalizes individual autonomy by allowing data subjects to decide whether and how their data will be processed. Yet decades of privacy research have documented the ‘notice-and-consent’ paradox: while organizations provide notice (privacy policies and disclosures), users rarely engage with these materials, and even when they do, cognitive constraints, time pressure, and information asymmetries limit comprehension. In mobile contexts, these constraints are intensified because screens are smaller, interactions are faster, and permissions are requested at moments when users are goal-driven (e.g., installing an app to complete a task). As a result, consent is often closer to acquiescence than to informed choice.

From a governance perspective, consent performs two additional functions. First, it provides a legal basis for processing that is relatively flexible for organizations. Second, it allocates responsibility: if the user consented, the user is presumed to have accepted the associated risks. This allocation is especially problematic in smartphone ecosystems because the ecosystem itself shapes what is practical to refuse. When refusing consent implies losing access to essential services (communication, banking, transportation), consent becomes coerced by dependence.

2.2 Smartphone Ecosystems and the Architecture of Data Flows

Smartphones differ from traditional web environments in their architecture and governance. They rely on operating systems (Android, iOS), app stores, and standardized permission models that mediate access to sensors and data. Applications increasingly incorporate third-party software development kits (SDKs) for advertising, analytics, and personalization. These SDKs can enable cross-app tracking and data sharing that is difficult for users to observe. In addition, background processes and persistent identifiers can generate continuous data flows even when an app is not actively used. Such ecosystem characteristics create opacity: users cannot easily map which actors access which data for what purposes.

The literature on mobile privacy highlights two recurring themes. The first is ‘permission fatigue’: repeated prompts lead users to accept requests quickly, often without evaluation. The second is ‘invisible processing’: data use for secondary purposes (profiling, behavioral targeting, inference) occurs beyond the surface interaction where consent is requested. These themes suggest that smartphone ecosystems are not neutral channels; they are governance environments that shape privacy outcomes through technical and interface design.

2.3 User Agency, Control, and Contextual Integrity

To rethink data protection, this paper draws on the concept of user agency: the capacity of individuals to understand, influence, and contest how their data are processed. Agency is not merely a psychological trait; it depends on infrastructures, interfaces, and institutional support. A control-oriented approach emphasizes ongoing rights and practical tools for managing data (e.g., review, revoke, limit, audit), rather than a one-time decision at the point of collection.

Contextual integrity provides a complementary theoretical lens by conceptualizing privacy as appropriate information flows relative to contextual norms. In smartphone ecosystems, data collected in one context (e.g., health, location, communication) may be repurposed in another (e.g., advertising, credit scoring), violating users’ contextual expectations even if a generic consent was obtained. This highlights why consent is insufficient: it often abstracts away from context, while privacy harms are context-dependent.

2.4 Research Gap and Conceptual Contribution

Existing scholarship has developed rich insights into mobile permissions, privacy perceptions, and regulatory compliance. However, three gaps remain salient. First, much of the literature still treats consent as the central point of intervention, rather than examining the deeper ecosystem structures that predetermine choices. Second, emerging economies such as Vietnam are underrepresented in theory-building, despite their smartphone-first trajectories and distinct governance capacities. Third, there is a need for integrative frameworks that connect regulatory instruments, platform/OS governance, and user-facing control mechanisms.

This paper contributes by reframing personal data protection in smartphone-centric ecosystems as a control problem and by articulating how Vietnam's context shapes the limitations of consent and the policy/design space for control-oriented governance.

3. RESEARCH CONTEXT: VIETNAM

Vietnam has experienced rapid digital transformation, with mobile connectivity and platform services playing a central role. Recent digital adoption reports indicate very high levels of cellular connectivity and extensive reliance on mobile internet access. Platform-mediated services—messaging, digital wallets, e-commerce marketplaces, and ride-hailing—are routinely accessed through smartphones, increasing both the volume and sensitivity of personal data processed.

3.1 Regulatory Landscape

Vietnam's personal data protection regime has evolved quickly. A key milestone is Decree 13/2023/ND-CP on Personal Data Protection, issued on 17 April 2023 and effective from 1 July 2023. Decree 13 clarifies responsibilities of personal data controllers and processors, sets out principles for processing, and specifies consent requirements (including that silence or non-response does not constitute consent). It also emphasizes rights of data subjects such as the right to know, right to consent and withdraw consent, and the right to request deletion or restriction, subject to legal conditions. In addition to Decree 13, Vietnam's cybersecurity-related legislation and sectoral rules interact with personal data governance, shaping compliance expectations and enforcement practices.

3.2 Market Features and Ecosystem Dominance

Vietnam's smartphone-centric ecosystem is characterized by strong concentration of operating system governance (Android/iOS), high dependence on app stores, and the presence of large domestic and regional platforms. These conditions shape privacy outcomes in three ways. First, users' choices are constrained by platform availability and network effects (e.g., messaging apps become essential due to social dependence). Second, platform operators can set privacy defaults and interface patterns at scale. Third, third-party advertising and analytics ecosystems remain influential, creating cross-service data flows that are difficult to control.

3.3 Why Vietnam Matters for Theory and Practice

Vietnam provides a theoretically relevant case because it combines rapid smartphone-led platformization with evolving regulatory instruments and practical enforcement challenges. Insights from Vietnam are likely to generalize conceptually to other smartphone-first, emerging governance contexts, while also offering locally grounded policy recommendations.

4. METHODOLOGICAL APPROACH

This study adopts a conceptual and contextual research design. Conceptual papers aim to develop integrative arguments, frameworks, and propositions by synthesizing existing theory and evidence. In this paper, the conceptual component is the shift from consent to control as a governance logic for personal data protection in smartphone-centric ecosystems. The contextual component uses Vietnam as a focal setting to identify how regulatory instruments and ecosystem conditions shape the feasibility and limitations of this shift.

The analysis combines three sources of input: (1) an integrative review of literature from privacy studies, information systems, and human-computer interaction on consent, mobile permissions, and user agency; (2) document analysis of Vietnam's regulatory instruments, with emphasis on Decree 13/2023/ND-CP; and (3) ecosystem-informed reasoning about smartphone architectures (OS permissions, app store governance, third-party SDKs) and typical user interaction patterns.

The analytic strategy proceeds in two steps. First, we identify and synthesize mechanisms that make consent ineffective in smartphone ecosystems (e.g., fatigue, opacity, dependence, and design manipulation). Second, we map these mechanisms to a control-oriented framework that specifies actionable levers at different governance layers (user interface, app-level controls, OS-level safeguards, and regulatory oversight). The outcome is a structured framework and a set of propositions that can be tested empirically in future work.

5. Analysis: Why Consent Fails in Smartphone-Centric Ecosystems

This section synthesizes key mechanisms through which consent-based personal data protection fails to deliver meaningful protection in smartphone environments. The mechanisms are presented as a structured set of failure modes that jointly undermine the assumptions of informed and voluntary choice.

5.1 Consent as Interactional Friction, Not Informed Choice

On smartphones, consent is typically encountered as friction in the user journey: an app requests permissions, a banner asks for tracking allowance, or a privacy policy is presented during registration. Because smartphone use is task-oriented, users often accept prompts to proceed. This produces a behavioral reality in which consent is not a considered decision but a micro-interaction optimized for speed. The normative implication is that legal consent does not reliably reflect user preference.

5.2 Information Asymmetry and the Opacity of Data Flows

Consent presumes that users can evaluate what data are collected, for what purposes, and by which actors. In practice, smartphone ecosystems are opaque. Permissions describe broad categories (‘location’, ‘contacts’, ‘microphone’) but seldom communicate secondary uses (profiling, inference, monetization) or third-party sharing. Data processing may occur in the background, via embedded SDKs, or through server-side analytics beyond the user’s observation. This opacity breaks the informational foundation of consent.

5.3 Permission Fatigue and the Normalization of Over-Collection

Repeated requests for permissions generate fatigue. Over time, users learn that refusal can disrupt functionality, while acceptance enables the immediate task. As fatigue accumulates, users become less selective. Organizations may also design applications to request more permissions than strictly necessary to maximize data extraction. The outcome is a structural drift toward over-collection.

5.4 Dependence, Network Effects, and the Illusion of Voluntariness

Consent is meaningful only when refusal is feasible. In smartphone ecosystems, refusal may entail exclusion from social and economic participation: messaging platforms are needed for work and social coordination; payment apps are needed for transactions; mobility apps support travel. Network effects and service dependence produce a context in which consent is formally voluntary but functionally coerced. This is particularly salient in smartphone-first economies, where alternatives may be limited.

5.5 Interface Manipulation and Dark Patterns

Consent is mediated through interface design. Dark patterns can nudge users toward acceptance through visual salience, default settings, time pressure, or confusing choices. Even when laws require ‘freely given’ consent, the practical ability to detect and enforce manipulative design is limited. In mobile interfaces, small screens and limited attention make users especially vulnerable to such nudges.

5.6 The Responsibility Shift: From Organizations to Individuals

Finally, consent-based governance can shift responsibility from organizations to individuals. When harms occur, organizations can claim that users consented, while users lack the tools to monitor, audit, or contest downstream processing. This responsibility shift is inconsistent with the asymmetry of power in smartphone ecosystems, where organizations and platform providers control the technical architecture.

Taken together, these mechanisms show that consent-based data protection is not merely imperfect; it is structurally misaligned with smartphone-centric ecosystems. A shift to control is therefore required to reduce reliance on individual cognition and to embed protections in system design and governance.

6. From Consent to Control: A Conceptual Framework

A control-oriented approach to personal data protection emphasizes ongoing manageability, transparency, and accountability rather than one-time agreement. Control should be understood across layers of the smartphone ecosystem: user-facing interfaces, application-level controls, operating system governance, and regulatory oversight. This section proposes a framework that operationalizes 'control' as a multi-layer governance construct.

6.1 Defining Control in Smartphone Ecosystems

Control refers to the practical capacity of users (individually and collectively) to influence data processing outcomes. It includes: (1) visibility (knowing what happens to data), (2) configurability (setting preferences and limits), (3) revocability (withdrawing access and triggering effective changes), (4) contestability (challenging misuse), and (5) accountability (ensuring actors face consequences for violations).

6.2 The Consent-to-Control Transition

The transition entails shifting the primary burden away from user comprehension at the point of collection and toward design-embedded safeguards and enforceable governance. Consent remains relevant but becomes one element among several controls, rather than the single foundation.

6.3 A Layered Control Framework

Table 1 summarizes the proposed framework, identifying key control levers, responsible actors, and typical implementation instruments.

Table 1. Layered control framework for personal data protection in smartphone ecosystems (Vietnam context)

Layer	Primary actors	Control levers	Illustrative instruments
User interface (UX)	Apps, platforms	Clear choices; friction-balanced design; anti-dark-pattern UI	Permission rationale; equal-salience options; privacy dashboards
Application level	App developers; platform operators	Data minimization; purpose limitation; in-	Granular toggles; local processing

		app controls	options; data export/delete tools
Operating system level	OS providers; device manufacturers	Permission architecture; runtime controls; cross-app tracking limits	Permission auto-reset; sensor indicators; per-app network access; SDK governance
Platform/app store level	App stores; platform governance bodies	Review and enforcement; SDK transparency; policy compliance	Privacy labeling; audits; removal of non-compliant apps; SDK disclosure requirements
Regulatory and oversight	State agencies; regulators; courts	Accountability; sanctions; standards; redress	Enforcement of Decree 13; guidance on valid consent; standardized privacy-by-design requirements

6.4 Propositions for Future Empirical Research

To guide subsequent empirical work in Vietnam and comparable contexts, the framework yields several propositions:

P1: In smartphone-centric ecosystems, higher opacity of data flows is associated with lower meaningfulness of consent and higher perceived loss of control.

P2: Stronger OS-level controls (e.g., granular permissions, cross-app tracking limits) strengthen user-perceived control and reduce resignation.

P3: When essential services depend on data-intensive platforms, users are more likely to provide consent despite privacy concerns, indicating functional coercion.

P4: Regulatory enforcement capacity moderates the relationship between formal consent requirements and real-world privacy outcomes.

These propositions illustrate how the conceptual contribution can be translated into testable hypotheses, without requiring the present paper to conduct a full empirical study.

7. Vietnam-Specific Implications and Feasibility of Control

This section situates the control-oriented framework within Vietnam's regulatory and market conditions, focusing on feasibility, constraints, and priority actions.

7.1 Operationalizing Decree 13/2023/ND-CP Beyond Formal Consent

Decree 13 strengthens Vietnam's personal data protection architecture by clarifying consent conditions and assigning responsibilities to controllers and processors. However, translating legal requirements into user protection requires operational guidance and enforceable standards. For example, consent validity depends on whether users are provided with clear, specific information and practical mechanisms to withdraw consent. In smartphone contexts, effective withdrawal must be technically implemented, not merely offered as a theoretical right.

7.2 Ecosystem Governance Priorities in Vietnam

Given the dominance of mobile platforms and the high reliance on a small number of ecosystem gatekeepers, Vietnam's privacy governance should prioritize system-level interventions with high leverage. These include: (1) standardized privacy notices optimized for mobile screens; (2) enforcement against dark patterns in permission and privacy interfaces; (3) transparency requirements for third-party SDKs and cross-app tracking; and (4) accountability mechanisms that enable audits and sanctions.

7.3 User Capabilities and Privacy Literacy

A shift to control does not remove the need for user capability. Instead, it reduces unrealistic expectations that users will read long policies and make optimal decisions. In Vietnam, improving privacy literacy remains important, but should be paired with simplified control interfaces and default protections that do not require advanced technical understanding.

7.4 Emerging Economy Considerations

Vietnam also illustrates challenges common to emerging economies: rapid innovation outpaces regulatory capacity, platform governance structures are evolving, and cross-border data processing complicates enforcement. Control-oriented approaches can help by embedding protections in technical architectures and platform governance, thereby reducing dependence on individual enforcement actions by users.

8. Implications

8.1 Theoretical Implications

This paper contributes to privacy and information systems scholarship by reframing personal data protection in smartphone-centric ecosystems as a control problem. It integrates insights from mobile privacy (permissions, fatigue, opacity) with governance perspectives (ecosystem gatekeepers, accountability) and contextual integrity to explain why generic consent fails in practice. The layered control framework provides a conceptual bridge between micro-level user experience and macro-level governance.

8.2 Policy Implications

For policymakers in Vietnam, the analysis suggests that strengthening consent requirements is necessary but not sufficient. Policy should also target the design and governance of ecosystems. Priority instruments include: (1) standards for mobile-friendly privacy notices and consent interfaces; (2) explicit prohibition and enforcement against dark patterns; (3) requirements for third-party SDK disclosure and auditing; (4) minimum OS-level protections (e.g., granular permissions, default minimization) for apps operating in Vietnam; and (5) accessible complaint and redress mechanisms for users.

8.3 Design and Managerial Implications

For platform operators and app developers, a control-oriented approach implies privacy-by-design and privacy-by-default practices that reduce reliance on user decisions. Practical measures include reducing permission scope, providing contextual explanations at the moment of data access, implementing dashboards that allow users to review and revoke permissions, and ensuring that withdrawal of consent triggers real changes in processing. Managers should treat privacy not only as compliance, but as a trust-building capability in platform markets.

9. CONCLUSION

Smartphone-centric digital ecosystems challenge the foundations of consent-based personal data protection. In Vietnam, where smartphones mediate a growing share of social and economic life, consent mechanisms are weakened by opacity of data flows, permission fatigue, service dependence, and interface manipulation. This paper argued that these problems are structural and proposed a shift from consent to control—a governance logic emphasizing ongoing manageability, system-level safeguards, and platform accountability.

The paper’s contributions include a synthesis of failure modes of consent in smartphone ecosystems, a layered control framework linking ecosystem layers to actionable levers, and a contextual analysis of Vietnam’s regulatory and market conditions. Limitations include the conceptual nature of the study and reliance on secondary sources; future research should empirically test the proposed propositions and compare Vietnam with other emerging economies. Nonetheless, the core implication is clear: meaningful personal data protection in smartphone ecosystems requires moving beyond the ritual of consent toward enforceable, user-centered control.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. Proceedings of the IEEE Symposium on Security and Privacy.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. Journal on Telecommunications and High Technology Law, 10, 273-307.

Decree No. 13/2023/ND-CP (Vietnam). (2023). Decree on Personal Data Protection (issued April 17, 2023; effective July 1, 2023). Government of Vietnam.

European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119-157.

Solove, D. J. (2021). The myth of the privacy paradox. George Washington Law Review, 89, 1-51.

Westin, A. (1967). Privacy and Freedom. Atheneum.

Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–52.

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI dark patterns and where to find them: A study on mobile applications and user perception. In Proceedings of the ACM CHI Conference on Human Factors in Computing Systems (CHI '20). https://doi.org/10.1145/3313831.3376600

Gunawan, J., Santos, C., & Kamara, I. (2022). Redress for dark patterns privacy harms? A case study. Computer Law & Security Review, 46, 105701. https://doi.org/10.1016/j.clsr.2022.105701

Isola, C., et al. (2025). A systematic literature review on dark patterns for the legal domain. Computer Law & Security Review.

Chen, M. (2025). Trust, privacy fatigue, and the informed consent dilemma in mobile app privacy pop-ups: A grounded theory approach. Information, 20(3), 179.

Australian Government, Digital Services Board. (2024). Patterns in the Dark: Deceptive design patterns and consumer harm (Report).

KPMG Vietnam. (2023). Legal alert on Decree 13 on Personal Data Protection. KPMG Vietnam.

EuroCham Vietnam. (2023). Decree 13/2023/ND-CP on Personal Data Protection (English translation). European Chamber of Commerce in Vietnam.

Wang, W., et al. (2025). An exploration of the influencing factors of privacy fatigue through a stressor–strain–outcome perspective. Scientific Reports.