Beyond the Wallet: Mapping Privacy Compliance in Ghana's Fintech Ecosystem

Abstract

This study examines data privacy compliance within Ghana's expanding financial technology (fintech) sector, where digital inclusion advances amid growing data governance gaps. Employing a mixed-methods design, it integrates policy analysis, technical inspection, and a user survey to assess adherence to the Data Protection Act (DPA). Findings reveal notable deficiencies in informed consent, data minimality, retention practices, and the clarity of user rights and disclosures. Security practices often fall short of the DPA mandates by prioritizing transit encryption over robust at-rest protections and regular testing. The study contributes an empirical framework to guide regulatory enforcement, enhance user awareness, and strengthen privacy governance in Ghana and comparable emerging digital markets.

keywords: Data Governance, Privacy, Ethics, Fintech, Mobile Financial Services

1 Introduction

The rapid growth of financial technology (fintech) services in Ghana has enhanced digital financial inclusion. This inclusion is built on the collection and processing of vast amounts of sensitive personal data, ranging from biometric information to real-time geolocation. Although Ghana's Data Protection Act, 2012 (Act 843) (DPA) [1] sets out principles for lawful processing, transparency, purpose limitation, and security, there has been limited empirical research on how fintech applications implement these requirements. This creates a critical need to move beyond policy-on-paper and scrutinize the on-device reality of data privacy to safeguard consumers and ensure the sustainable, trust-based growth of Ghana's digital economy. In this study, we establish an empirical benchmark for evaluating and enhancing data privacy practices within Ghana's and by etension, Africa's burgeoning fintech ecosystem. This paper (RQ1) systematically analyzes the stated data practices and privacy compliance of Ghanaian fintech apps through policy evaluation; (RQ2) technically inspects the data access and transmission behaviors of these apps using static and dynamic analysis; and (RQ3) assesses Ghanaian users' perceptions, expectations, and concerns regarding privacy in fintech platforms.

This study provides a methodology for auditing digital privacy compliance in an emerging African market. It maps the privacy landscape of Ghanaian fintech and empirically validates the gap between policy, practice, and user perceptions. The impact is threefold: it equips the Data Protection Commission (DPC) with evidence for enforcement; empowers Ghanaian consumers with the knowledge to make safe digital choices; and provides a framework for privacy advocates across the Global South, ultimately fostering a more transparent and trustworthy digital financial ecosystem.

2 Method(s)

The study draws on Nissenbaum's [9] contextual integrity framework, conceptualizing Ghanaian fintech apps as "information flow systems" to examine relational data-sharing practices among users, providers, third parties, and state actors. We adopt a mixed-methods [5][7] approach to audit leading apps, comparing stated policies, observed data practices, and user privacy norms. From 63 Bank of Ghana (BoG)–approved fintechs, we selected the top 20 by aggregating download metrics from the Apple and Google Play stores. Their privacy policies and terms of service were collected and analyzed using content analysis [10] informed by the DPA's requirements to evaluate clarity, scope, and legality. We conducted static analysis to identify app permissions and embedded third-party trackers, followed by dynamic sandbox testing to observe real-time data flows, including what data are transmitted, to whom, and under what conditions. An online survey using factorial vignettes [8] assessed user acceptance of data-sharing scenarios, complemented by semi-structured interviews exploring user perceptions of privacy and consent.

3 Results and Discussion

Our analysis suggests pervasive compliance gaps. Most apps rely on "sole-purpose" consent clauses buried in lengthy terms of service. While most fintech firms cite the DPA as their primary legal framework, many continue to rely on browsewrap [6] or implied consent models, a practice that conflicts with the DPA, which stresses the importance of informed consent and the data subject's right to object. Data collection policies indicate a recurring pattern of over-collection, as exemplified by the gathering of location data, SMS logs, and contact lists that exceed what is strictly necessary for financial transactions. This potentially breaches the Principle of Minimality under the DPA. User rights provisions show significant inconsistency across platforms. While some platforms explicitly enumerate comprehensive rights such as access, correction, and erasure, others omit key entitlements, including data portability and the right to be forgotten, both central to the principles of rectification and erasure as required by the DPA. Similarly, retention practices, such as a a platform's ten-year data retention policy, conflict with the DPA's stipulation that data be retained no longer than necessary. The analysis further showed that security measures as stated in the policy often cover only data in transit (e.g., SSL encryption) rather than encompassing the full range of technical and organizational safeguards envisioned by the DPA. Data disclosure practices demonstrate limited transparency, as exemplified by some platforms' omission of a disclosure section entirely, thereby failing to meet the specification of purpose requirement outlined in the DPA.

A significant 85% (17 out of 20) of fintech platforms in Ghana provide contact information in their privacy policies as a mechanism to address user concerns. The 15% that omit this information pose a significant barrier to users wishing to exercise their rights under the DPA. Email emerges as the universal standard for communication, reflecting the dominance of digital channels communications. In contrast, multi-channel support is less common. Only 30% provide a phone number and 25% list a physical address, suggesting a "digital-first" but potentially less accessible grievance process for non-technical users. Among fintechs that provide email addresses, 58.8% use a Dedicated email (e.g., privacy@company.com or something similar). This indicates that more than half of these firms have established a specialized channel for data protection, while the remaining 41.2% likely funnel privacy inquiries through general support queues. There is a notable mix of Local vs. Foreign presence. Of the policies that specify a location, there is a tilt toward Local (62.5%) over Foreign (37.5%) entities.

Cross-border data flows to cloud providers in jurisdictions without adequacy decisions are often undisclosed, contravening the DPA's safeguards. Security practices vary; While some apps employ TLS for data in transit, few implement encryption at rest or conduct regular penetration testing, despite Act 843's mandate for reasonable security measures. The regulatory landscape appears fragmented. BoG licensing requirements focus on AML/CTF and financial stability, with limited explicit references to data protection compliance. The Stock Exchange's (GSE) oversight of investment-tech platforms includes disclosure of obligations but lacks harmonization with teh DPA. Consequently, fintechs face divergent compliance checklists, leading to "regulatory fatigue and selective adherence. At the user level, there is consensus that the DPC's limited enforcement capacity stems from budgetary constraints and low public awareness. This reduces the perceived cost of non-compliance. While consumer rights analyses stress the need for "privacy-by-design" [11] culture, fintech companies are often contrained by rapid product-release cycles [2] [3] and ambiguous guidance [4] as barriers to full compliance with data protection requirements.

4 Conclusion

This work in progress reveals a systemic shift where "Notice" has superseded "Active Stewardship." The industry broadly struggles with the Principle of Minimality, often justifying excessive collection of GPS and contact data as "operational necessity". Legal adherence is frequently performative; for instance, citing the Act while employing "browsewrap" models bypasses the granular consent spirit of data protection. Ultimately, the transition from simple transparency to full accountability remains incomplete. To achieve true compliance, Ghanaian fintechs must move from "implied" to "explicit" user-centric governance.

References

[1] Ghana data protection act 2012 (act 842), 2012.

[2] Fintech Regulatory Challenges: Navigating Compliance in 2025 - Nico Halle & Co. Law Firm, July 2025.

[3] Jo Ann Barefoot. Modernizing Consumer Financial Regulation For the Digital Age, June 2020.

[4] Otieno Geoffrey and Kiraka Ruth. Navigating the Regulatory Labyrinth: Compliance Dilemmas and Lead User Innovation in the Fintech Sector. *Proceedings of the International Conference on Business Excellence*, 18(1):2581–2593, 2024.

[5] Kirstie Hawkey. Privacy research: A mixed methodology approach. In *Proc. of Workshop on Privacy and HCI: Methodologies for Studying Privacy Issues, CHI'06*, 2006.

[6] Nancy S Kim. *Wrap contracts: Foundations and ramifications*. OUP Us, 2013.

[7] Ying Li, Rui Yang, and Yikun Lu. A privacy risk identification framework of open government data: A mixed-method study in china. *Government Information Quarterly*, 41(1):101916, 2024.

[8] Kirsten Martin and Helen Nissenbaum. What is it about location? *Berkeley Technology Law Journal*, 35(1):251–326, 2020.

[9] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[10] Ganesh B. Regulwar, Ramachandro Majji, Santosh Kumar Kottu, Anvesh Kachi, and Ranjith Reddy Sureddy. Content analysis and visualization of privacy policy using privacy management. *AIP Conference Proceedings*, 2942(1):020013, 02 2024.

[11] Alex Rizzi. Embedding Trust: The Potential of Privacy by Design for Inclusive Finance, December 2022.