Reconsidering Competition and Privacy Overlaps in Kenya

Competition law and data privacy are at the core of shaping our digital economy. These two concepts are "nuanced and multifaceted,"[1] with emerging interactions. This has been observed in Kenya, particularly in the fintech sector, which is one of the least regulated sectors in the country.[2] Currently, the sector is governed by Kenya's existing regulatory framework for financial services, which exempts certain firms from regulation.[3]

Kenya enacted the Data Protection Act 2019 as the primary data protection framework, significantly altering the way fintech data is processed, as fintech services rely on personal data processing. The Data Protection Act has implications for businesses, particularly as it pertains to legal and technical compliance measures and data processing. Consumer protection is central to any organization that collects or processes personal data about its customers. Consumers are considered data subjects under data protection law – "identified or identifiable natural person who is the subject of personal data."[4] The Act establishes consumers' rights to their personal data, businesses' obligations to consumers, and, most importantly, the practical steps and data processing principles that businesses should follow and adhere to in order to implement these rights and obligations.[5]

---

[1] Erika M. Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy', Report to the Global Privacy Assembly Digital Citizen and Consumer Working Group, July 2021.

[2] Dominic Indokhomi and Ariana Issaias, 'Opportunities and Pitfalls in Fintech Regulatory Push', Business Daily, 26 April 2021, https://www.businessdailyafrica.com/bd/opinion-analysis/columnists/opportunities-pitfalls-in-fintech-regulatory-push-3376510.

[3] Indokhomi and Issaias.

[4] Section 2, Data Protection Act 2019.

[5] The Data Protection Act applies to all businesses in Kenya that qualify as either a data controller or processor pursuant to Section 2 of the Data Protection Act. The Act recommends that inspections and routine assessments of regulated businesses be supervised by the Office of the Data Protection Commissioner, which is responsible for the enforcement of the Data Protection Act. Additionally, and in light of recent developments, the Officer of the Data Protection Commissioner has issued additional guidelines that supplement the Act and clearly outline the various procedures, requirements that must be adhered to, and consequences for non-compliance. These frameworks have influenced internal business changes, such as new policies and systems, enhanced data protection measures, and increased internal training and awareness.

There has been a renewed interest in and ongoing discussions about competition law and privacy, owing in part to the growth of the digital economy and competition.[6] Global research and commerce, as well as social media platforms, continue to dominate the digital market and economy, raising concerns about cross-border data transfers and consumer privacy. Digital lending apps and the regulation of the fintech sector have garnered particular attention in Kenya. According to a study on privacy and digital lending apps in Kenya, digital lending apps rely on processing of personal data in addition to location-based services.[7] These digital lending apps are economically significant, making them a priority for competition law, and privacy-sensitive due to their processing of personal data and access to location. The discussions about regulation, competition law, and consumer protection, highlight existing legislation and the need to adequately address realities of digital competition.[8] This calls for improved coordination and collaboration between competition and data protection authorities when it comes to regulating digital platforms and the digital economy in general.

Apart from these legal and policy concerns, there is growing interest in sandboxing in the fintech industry. A recent sandbox consultation document expressly states that 'regulatory nimbleness, flexibility and responsiveness provided by *principle-based* regulation is even more important in the FinTech sector where thriving innovation is the lifeline of a vibrant business enterprise.'[9] Where it comes to data protection in the fintech space, regulation continues to lag behind technological advancements,[10] although this is certainly to be expected and not necessarily bad for the various stakeholders. Nevertheless, due to the lack of a comprehensive fintech-specific legal

---

[6] Vellah Kedogo Kigwiru, 'Enforcing Competition Law and Consumer Protection During the COVID-19 Pandemic in Africa: The Competition Authority of Kenya', *Competition Policy International* (blog), 5 August 2020, https://www.competitionpolicyinternational.com/enforcing-competition-law-and-consumer-protection-during-the-covid-19-pandemic-in-africa-the-competition-authority-of-kenya/.

[7] Centre for Intellectual Property and Information Technology Law (CIPIT), 'Privacy and Data Protection Practices of Digital Lending Apps in Kenya', 2021.

[8] Kigwiru, 'Enforcing Competition Law and Consumer Protection During the COVID-19 Pandemic in Africa'.

[9] Capital Markets Authority, *Stakeholders' Consultative Paper on Policy Framework for Implementation of a Regulatory Sandbox to Support Financial Technology (Fintech) Innovation in the Capital Markets in Kenya* 2.

[10] Dr Anton Didenko, 'Regulatory Challenges Underlying FinTech in Kenya and South Africa', December 2017, 7.

framework, the industry is governed by a number of statutes, including the Competition Act and the Data Protection Act. There are existing gaps in the regulation of both competition and data privacy. This necessitates identifying existing gaps and areas of overlap in order to ensure effective regulation while also achieving the common goal of consumer protection.

Without a doubt, privacy is at the core of the digital economy. Competition and privacy enforcement demonstrates that there are shared policy objectives in the digital economy, with the primary goal of protecting consumers while ensuring their privacy. This requires collaboration between the two areas of law and their respective regulatory authorities in order to develop unified and comprehensive enforcement strategies that adequately address digital competition, existing gaps, and overlaps between the two areas of law.