**Microcredit and fintech: are consumer rights and data protection sufficient?**

Microcredit, which broadly describes the provision of small loans to those with limited access to formal financial services particularly for self-employment ventures, has been a key response to poverty globally. The intellectual advocate of this scheme in its modern form, Yunus, claimed in his book, [Banker to the Poor](https://www.publicaffairsbooks.com/titles/muhammad-yunus/banker-to-the-poor/9781586485467/), that an increase in microcredit corresponds directly to a decrease in poverty. His claim that credit is a human right galvanized the birth of the microcredit industry in 1977 and became the basis for Yunus’s Nobel Peace Prize in 2006.

Today, African countries are pace setters in using fintech to make microcredit more accessible to millions of Africans. [Defenders of microcredit](https://www.dw.com/en/microfinace-supporters-defend-yunus-legacy/a-15102807) argue that it has an impact on improving the daily lives of people by funding daily needs, rather than for business loans, as originally envisioned. While these claims feed into the idea of freedom and agency for people, the high cost of microcredit through high interest rates makes it hard to distinguish practices of predatory loan sharks from reputable fintech companies. In many African countries, microcredit practices are not fully regulated, creating further profitable opportunities for lenders to prey on creditors forced to live on the margins. This dichotomy is precisely what this note seeks to interrogate by contributing a response to WISER’s research initiative on the extent to which African data protection agencies are aware of, interested in, and engaging with issues such as fintech and e-commerce.

Fintech’s primary financial product in Africa, mobile lending, uses algorithms to mine people’s devices to assess their creditworthiness. While lending algorithms are closely guarded secrets, existing research shows that fintech corporations believe ‘[all data is credit data](https://journals.sagepub.com/doi/abs/10.1177/1024529417712830)’ leading fintech companies to capitalize on poor people’s debt and data. The discriminatory impact of data mining by fintech companies is enormous. As Pasquale, the author of [*The Black Box Society*](https://www.hup.harvard.edu/catalog.php?isbn=9780674970847) puts it, ‘you can get in a death spiral simply by making one wrong move, when algorithms amplify a bad data point and cause cascading effects.’ A case study from Nigeria puts this in perspective.

*Privacy breaches and predatory practices in Nigeria’s fintech industry*

In a recent [report](https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html) released in December 2021 by an investigative journalism unit in Nigeria, Premium Times, there is a rise of fintech companies providing microcredit and these companies are resorting to “unprofessional measures of harassment, cyberbullying and breach of data privacy of their customers who may have defaulted in loans repayment.” For one of the companies profiled in the report, 9credit, the company’s [privacy policy](https://app-api.9moni.com/wap/agreement?name=register&system=9Credit) requires customers to consent to the manipulation of personally identifiable information and authorizes the company to “use collected data for purposes of collections (e.g. communicate with your phone-book contacts to finish collection when you are (sic) failed to repay.”

The Premium Times report revealed that fintech companies in Nigeria use underhand practices to make their customers default on loans to trigger and collect financial penalties on already high interest loans. These companies require customers to download their mobile application, which is used to gain unrestricted access to personal data on a customer’s phone. Apparently, when a customer defaults, these companies use their unrestricted access to the phone book contacts of their customers to send threatening messages and allege that the defaulting customer has listed the contact as a surety for the microcredit.

One of the fintech microcredit providers, Soko Loans, was the subject of an investigation by National Information Technology Development Agency (NITDA), the regulator responsible for the enforcement of Nigeria’s Data Protection Regulation. According to NITDA in the release of its [findings](https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/), action was taken against the company for “unauthorized disclosures, failure to protect customers’ personal data and defamation of character.” NITDA’s investigation revealed “complainants’ contacts who were neither parties to the loan transaction nor consented to the processing of their data confirmed the receipt of threatening messages.” Despite NITDA’s order for it to cease such practices, Soko Loans ignored the order and simply rebranded and directed customers to pay into its other business accounts.

NITDA has [acknowledged](https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/) that given the lack of cooperation from fintech companies and their failure to pay fines or implement sanctions imposed on them, a different enforcement strategy is needed especially with NITDA having nine active investigations against fintech companies. One of the new strategies is for NITDA to collaborate with the Federal Competition and Consumer Protection Commission to handle joint investigations, enforcement and possible prosecution of personal data breaches by fintech companies.

This approach is an attempt to fill a regulatory gap in Nigeria where there is no data protection law and the regulatory powers of NITDA as the oversight body to enforce the existing data protection regulation [has been questioned](https://esq-law.com/six-6-reasons-the-ndpr-must-be-quickly-replaced-olumide-babalola/). While the adoption of a data protection law alongside a regulator with enforcement powers may help in addressing the predatory practices within the fintech industry, the reality is other African countries with data protection laws and powerful regulators in place are also facing similar challenges.

In South Africa where microcredit thrives, the Credit Regulator has described the levels of unsecured lending as [unsustainable](https://www.tandfonline.com/doi/abs/10.1080/03056244.2018.1546429?journalCode=crea20). In 2017, the Credit Regulator approached the Human Rights Commission on ways to collaborate in investigating the rights based violations relating to unsecured microcredit and the predatory practices of lending companies. This resulted in the publication of a [human rights report](https://www.sahrc.org.za/home/21/files/SAHRC%20BHR%20RA%203%20-v3.pdf) on unsecured lending in South Africa. This means we need to generate new ways to address how systems such as fintech and microcredit, violate data protection rights and work to entrench poverty rather than alleviate it.

*Looking forward*

In response to the global hegemony of finance capital that is fueled by predatory lending and rising debt, countries such as Sri Lanka have explored [alternative finance models](https://www.cadtm.org/Microfinance-has-been-a-nightmare-for-the-global-south-Sri-Lanka-shows-that) such as affordable rural credit based on the history of cooperatives in the country. Recognising the current corporate structure of profit maximization is broken and driving the trends in fintech, it is important to develop alternatives to corporate financing that are beholden to institutional investors and passive capital. Such alternative models require innovative policy responses and are crucial for social mobility. By studying various approaches to existing models of alternative financing, we will be able to identify anti-models that are not working, those requiring further exploration and new ideas on alternative financing.

Fola Adeleke