February 2021

Digital Lending:

Inside the Pervasive Practice of LendTechs in Nigeria

Ikigai Innovation Initiative

TECH HIVE ADVISORY

regcompass

Naijasecforce

Acknowledgement

This report is based on an actual investigation using openly available information and open source tools. Our findings does not constitute a review of the legitimacy or otherwise of the practices detected. The report is based on analysis done between **10th – 29th August 2020**. The report is a collaboration between Tech Hive Advisory, NaijaSecForce, Regcompass and Ikigai Innovation Initiative. We also acknowledge those who provided information about their experience using some of the digital lending tools and everyone that contributed to this report.

Disclaimer

We have deliberately left out the service providers' names because it is not materially relevant to this report. It is not our intention to discredit or validate the practices investigated but raise awareness about the subject of this report. The report did not attempt to confirm the existence of the LendTechs identified with the Corporate Affairs Commission (CAC) or verify the identity of the promoters of the LendTechs.

Objective

This report aims to take an expository dive into the world of digital lending in Nigeria from a privacy, security and consumer protection viewpoints. The study will examine various issues such as data protection and privacy rights of users, security standards implemented by digital platforms, arbitrary interest rates, use of emerging technologies, and dark patterns. Finally, the report recommends improving consumer security, privacy, and, more importantly, regulating Nigeria's digital lending space.

Contributors

Victoria Adaramola
Favour Borokini
Musa Omayi
Oluwagbeminiyi Ojedokun
Tojola Yusuf
Mallick Bolakale
Moses Faya
Aishat Salami
Rita A. Chindah
Opeyemi Kolawole
Ayodeji Sarumi
Ridwan Oloyede
Nurudeen Odeshina
Other Anonymous Contributors

About Partners

Ikigai Innovation Initiative

Ikigai Innovation Initiative is a non-profit organisation set up to become the one-stop centre for Africa's technology policy. We promulgate diverse research on technology policy and legal frameworks across Africa. We also engage relevant stakeholders around the intersection of law, business and technology and advocate for better policies for the ecosystem at large.

Being a research centre focused on emerging technologies, policy and research, we often collaborate with leading research institutes, academia, organisations, civil society, and individuals on policy affecting technology. We also publish and contribute to whitepapers, reports, policy briefs, infographics, guides and guidance, academic journals and publications.

Our researchers work closely with government, stakeholders and ecosystem players, placing evidence and academic intuition at the heart of policymaking. lives and promoting digital rights and digital ethics. We bring together the latest insights, evidence and commentary from our researchers with our one-stop-shop vision for policy by connecting policymakers, decision-makers, and practitioners with our industry-leading research.

We also deliver an evidence-based policy that meets the grand challenges facing society by advocating for social justice in the face of technology; sensitisation of the public on technology policies that impact their rights and and lives and promoting digital rights and digital ethics.

NaijaSecForce

We understand how daunting it may be to get into the information security field or find a niche for yourself after learning the ropes. NaijaSecForce provides a platform for newbies and experts to interact in a mutually respectful space, openly share ideas and research materials and provide technical guidance for ethical hacking, cryptography, cyber risk management, and reverse engineering, cloud security and malware analysis. We meet monthly to discuss and share knowledge, ideas, threats and intelligence.

We also organise a yearly NaijaSecCon Conference. Nigeria Cybersecurity Conference (NaijaSecCon) is Nigeria's first of its kind 100% annual technical Cybersecurity Conference that uniquely merges information about the latest and relevant threats from a Nigerian context with live technical demonstrations and hands-on workshops.

Annually, NaijaSecCon attracts over 300 cybersecurity professionals from various industries including Financial Services, Insurance firms, Telecommunications, Oil and Gas, conglomerates, Tech Start-ups, Financial Technology (FinTech) companies, other privately-held organisations and also government Ministries, Department and Agencies (MDAs).

Contact: info@naijaseccon

About Partners

Regcompass

Regcompass Consults is a regulatory compliance and business advisory outfit that leverages technology to provide State of the art advisory services to startups and other tech companies. Formed with business and innovative insights into companies' challenges in the modern world by lawyers and technical experts, Regcompass is designed for brands and companies with regulatory compliance needs. We serve operators from various industries, especially within the tech ecosystem, ranging from financial services to gaming, health, media and tourism.

With our innovative approach to regulatory compliance and our vast experience in seamlessly navigating the unique business and regulatory terrain across various jurisdictions in Africa, we envisage our clients' needs and provide the best and most cost-effective way of meeting these needs.

Regcompass has the reputation of providing additional support like training its clients on Anti-money Laundering/Combatting the financing of terrorism training. We are looking forward to transforming the technology landscape with our innovative approach to business, compliance and regulatory advisory. As part of our core culture, we work with our clients to develop bespoke solutions to their various challenges. This unique attribute sets us apart from existing service providers. We are not just consultants; we are business-minded and highly focused professionals.

Contact: hello@regcompass.com

Tech Hive ™

Tech Hive Advisory Limited is a technology advisory firm that provides advisory and supports services to private and public organisations regarding the intersection between technology, business, and law. We focus on how emerging and disruptive technologies alter and influence the traditional way of doing things while acting as an innovation partner to our clients. These new technologies often birth new challenges requiring regulations to balance the benefit of innovation and users' rights and freedoms. Our experience and capability extend across startup advisory, privacy and data protection, data ethics, cybersecurity, intellectual property management and emerging technologies. We ensure our advice serves our clients well by having an excellent understanding of their business and the markets in which they operate.

Contact: contact@techhiveadvisory.org.ng

Abbreviations

Ads – Advertisement

AML- Anti Money Laundering

App – Mobile Application

CBN – Central Bank of Nigeria

CBK – Central Bank of Kenya

CFT - Counter-Terrorism Financing

CSP - Content Security Policy

DPIF – Nigeria Data Protection Implementation Framework

DPO – Data Protection Officer

Email - Electronic Mail

FCCPA – Federal Competition and Consumer Protection Act

FCCPC – Federal Competition and Consumer Protection Commission

FDCPA - Fair Debt Collection Practices Act

FinTech – Financial Technology

HTTP - Hypertext Transfer Protocol

KYC - Know Your Customer

LendTech – Lending Technology

NDPR – Nigeria Data Protection Regulation

NITDA – National Information Technology Development Agency

SMS - Short Messaging Service

SSL - Secure Socket Layer

SQL - Structured Query Language

RP - Referrer Policy

XSS - Cross-Site Scripting

Table of Content

Executive Summary

Lending Technologies (LendTechs), which are digital platforms that offer loan services and more, have witnessed increased use in recent years. This has been determined to be due to varying factors that may include stringent conditions to access credit from orthodox financial institutions (banks), less formal documentation and seemingly flexible credit terms. Despite the immense benefit, the rise in the use of these LendTechs poses various data protection, human rights, debt recovery harassment, consumer protection, privacy and security, and unfair contractual challenges. Another challenge identified is the lack of regulatory oversight on their operations, especially those operating with respective state governments' licenses. In today's climate, it has become increasingly necessary to ensure that sufficient steps are taken to protect consumers. LendTechs are expected to act responsibly and within what is permissible and not resort to predatory practices rife in the digital lending space.

In today's climate, it has become increasingly necessary to ensure that sufficient steps are taken to protect consumers

This report explored the world of LendTechs and examined the trends in LendTech applications and websites, legal and regulatory frameworks, operating models as well as the issues around data protection, use of emerging technologies, debt recovery, privacy, use of dark patterns, consumer protection and security practices adopted by LendTechs. It does so by examining 22 (Twenty-Two) LendTech mobile applications (Android OS) and websites (where it exists) for privacy and data protection compliance, reviewing their respective privacy notices and terms of use, analysing 10 (Ten) of the mobile applications for security compliance and obtaining information from LendTech users through interview.

Our findings show that some of the LendTechs violate the data protection and privacy rights of users. There is the pervasive use of unfair contractual terms in their terms of use. There are varying uses of emerging technologies like machine learning and artificial intelligence with minimal evidence of transparency with the Users, a data protection impact assessment or algorithm auditing. Besides, the use of dark patterns were observed with the purpose of manipulating Users into making decisions favourable to the LendTechs.

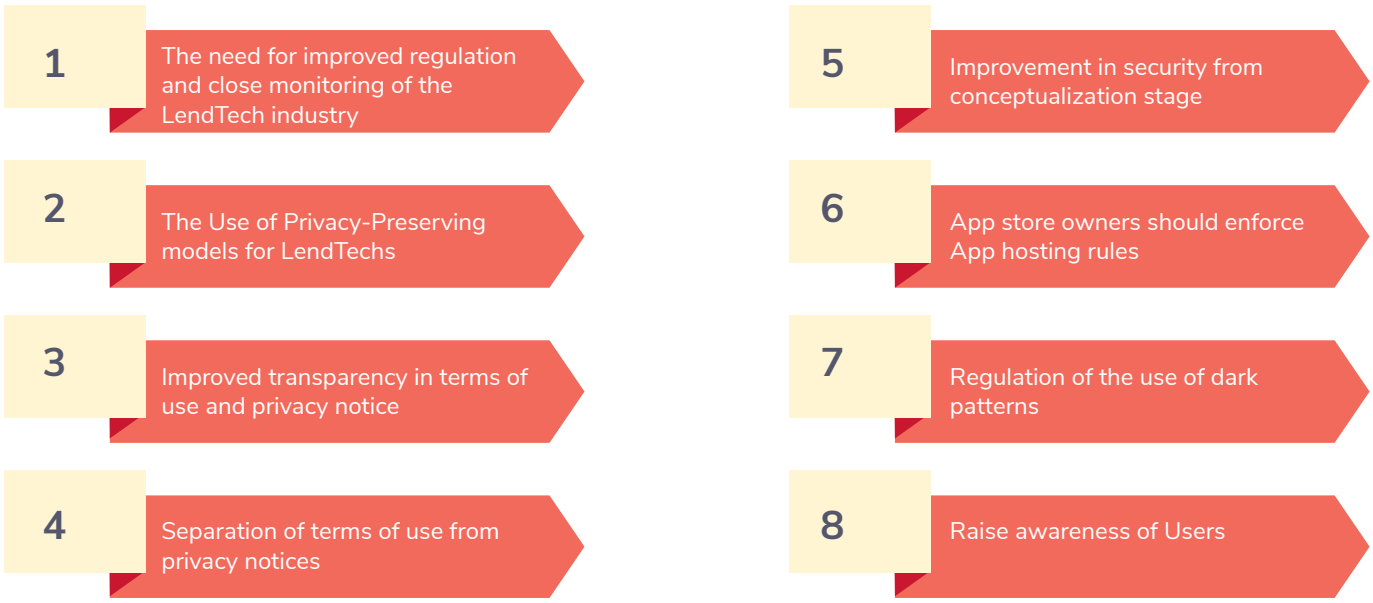
Summary of findings:

The report shows the concerns around the use of LendTechs, which include:

- 23% of the Apps used the dark pattern to manipulate Users;
- 60% of the apps reviewed have weak or poorly implemented encryption algorithms, which can endanger the mobile application's data storage and transmission;
- 64% of the apps reviewed did not prompt Users to read their Terms of Use before signing up;
- We found Seven (7) of the LendTechs using machine learning or artificial intelligence for their proprietary credit scoring and credit risk assessment algorithm, which decides on a User's suitability for a loan or otherwise. However, only one (1) provided information in its privacy notice about its existence contrary to the requirement of the law;
- 2 of the LendTech we made a data subject access request to did not acknowledge or respond to the request;
- 65% of Apps had advertising trackers embedded in them without notifying Users of their existence. All the Apps with Ads trackers examined lacked a mechanism to opt-in and opt-out of third-party tracking. None of them provided a straightforward way to opt-out of the services;
- 68% of the mobile applications did not have their privacy notice conspicuously visible to the Users. 18% of the Apps did not have a privacy notice, while 40% had incomplete or insufficient information in their privacy notice;
- We found instances where debt recovery relied on the threat of social disgrace and false allegation of crime against Users;
- We found a lot of cases in which contacts on the phone of Users received messages from LendTechs about the indebtedness of third-parties without the appropriate lawful basis and contrary to the requirement of the law;
- We found the use of unfair, unreasonable and unjust contract terms in terms of use;
- We found instances where LendTechs used auto-generated terms of use and privacy notice that did not reflect their processing activities and nature of services; and
- We found cases of LendTechs sending unsolicited marketing emails to non-users without their consent.

At the end of the report, we made the following recommendations:

- The need for improved regulation and close monitoring of the LendTech industry;
- The use of privacy-preserving models for LendTech applications and websites;
- Improved transparency in terms of use and privacy notice to genuinely reflect what they do;
- The separation of terms of use from privacy notices;
- Improvements in security from the conceptualization stage;
- App store owners should enforce their App hosting rules and kick out Apps that fail to meet the minimum standard;
- Regulation of the use of dark pattern; and
- Raising awareness of Users.



In conclusion, some of the LendTechs' irresponsible practices need to change to make LendTechs a responsible platform for credit access in Nigeria. Therefore, quick and lasting changes must be made to LendTechs; a responsive regulation will minimise Users' risk without stifling innovation and the potential benefit inherent in their services.

"User" and "Consumer" are used interchangeably to mean the borrower.

Methodology

This report considered both primary and secondary resources. It examined LendTechs' mobile applications (Android available on Google Play store) and websites offering credit facilities to Nigerian users. The selected LendTechs were analysed for adherence to data protection, cybersecurity, and consumer protection framework. The mobile applications and websites were investigated in a static state. [1] The analysis reviewed the selected mobile applications and websites by observing permissions, trackers, third-party requests, use of dark patterns, privacy notices, terms of use, and safeguard mechanisms adopted to protect users. The research also considered the legal framework for digital lending in Nigeria to verify these LendTechs' compliance with Nigerian laws and international best practices.

This report examined 22 (Twenty-Two) LendTech mobile applications and websites (where it exists) for privacy and data protection compliance, including reviewing their respective privacy notices and terms of use, and the use of dark patterns. We analysed 10 (Ten) of the mobile applications for security compliance. Only the website and mobile application version (Android OS where available) were appraised. Some users were also interviewed as part of this research. The research relied on open source tools and frameworks for the findings.

22

Mobile Applications & Websites

10

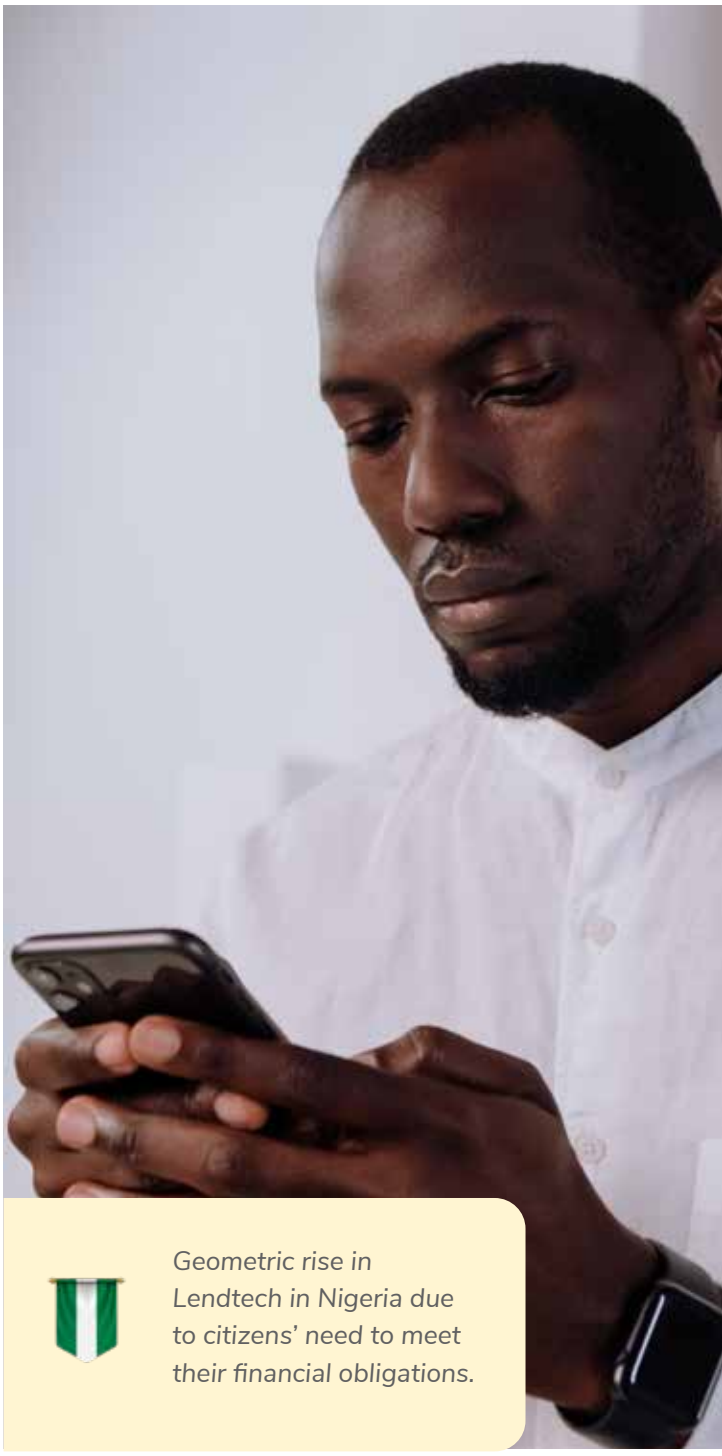
Mobile Applications for security compliance

Introduction

Access to credit facilities is a challenge in many developing countries, including Nigeria, with stringent formal documentation requirements, the near absence of quick micro-credit, [2] high-interest rates, the strict need for collateral alongside strict credit terms; all posing barriers to obtaining credit from traditional lenders (banks). [3] The resultant vacuum means borrowers often have to resort to informal lenders or schemes, which are poorly regulated and often have geographical limitations.

The limitations of both traditional and informal lending schemes and the existence of a flawed and redundant credit rating system in frontier markets created a gap. They birthed a veritable marketplace for digital lenders, who can provide quick loans with flexible tenor, [4] zero collateral, little or no documentation, and without geographical barriers across the country. The popularity of these digital lending platforms offering quick loans through mobile or web applications or third-party agents has seen a geometric rise in Nigeria due to citizens' need to meet their financial obligations. The increase eases access to credit with less formality than traditional lending institutions. [5]

While the above benefits appear exciting, the world of digital lending is not all rosy. There are verifiable reports of vaguely-worded terms of use, arbitrary interest rates, pervasive and gross privacy violations, weak security and unethical debt recovery practices employed by some digital lenders. This continuing predatory and pervasive practice has kept some consumers in perpetual debt through cut-throat interest rates and vague terms, whilst the threat of social disgrace is held over defaulters. [6]



Geometric rise in Lendtech in Nigeria due to citizens' need to meet their financial obligations.

The Rise of Digital Lending Platforms in Nigeria

The growth in the Nigerian Fintech space is witnessing increased investment, of which LendTech is a subset. [7] They typically operate using any of the models described below. The growth is fuelled by increased investor funding and the available market of users requiring quick financial aid. A quick search on Google Play Store provides a long list of the service providers who offer quick credit facilities with lesser formalities and zero documentation than traditional banks targeting consumers in Nigeria.

Despite an addressable credit problem and the immense benefit created by LendTechs, some providers have deployed a predatory and arbitrary model. Some of the platforms have low transparency with their terms of use and privacy practice, fail to implement sufficient security mechanisms, misrepresent the quality of service, manipulate users through dark design, and violate consumer rights with their invasive customer acquisition practice by sending unsolicited emails and SMS. Besides, State government agencies do not exercise sufficient regulatory oversight on the operations of licensed LendTechs. Their licensing rules ignore these challenges, which leaves consumers without protection and to the whims of operators.

In an extreme scenario, LendTech apps operations were reported to be responsible for “debt traps and suicide” in Kenya [8] and India [9] [10] , which prompted the Central Bank of Kenya (CBK) to issue a draft Regulation. [11] In Kenya, it was reported that “digital borrowing has become a social menace responsible for suicides, divorce, family breakups and increased listing of loan defaulters by the Credit Reference Bureau (CRB)”. [12] In India, there are reports of some of the LendTechs operating on the App market without licensing. [13]

Legal and Regulatory Regime of Lending Technologies ("LendTechs") in Nigeria

LendTech is the use of technology to provide various credit products to customers. Providers usually adopt technology tools to analyse customers' financial behaviour and generate credit ratings to determine whether a particular customer is eligible for a loan. LendTechs provide speedy loans within minutes and a quick credit scoring by accessing smartphone data such as call logs, bank SMS alerts, bill payment receipt, personal SMS, payment information, transactions data, e-commerce, search history, social network data, voice, airtime, e-money usage and other data that is often processed by computerised algorithms to determine credit eligibility.

They emerged to reach the under-served population to whom commercial bank loans are out of reach, in providing short-term loans.

In Nigeria, technology is not precisely regulated; however, the uses to which technologies are put have traditional regulations and governing laws. For instance, a company looking to carry on lending business must acquire the requisite license for its operation.

There are different licensing models for lending companies in Nigeria. As such, what businesses typically do is to research which model suits their business operations, bearing in mind their jurisdiction of operation and their capital.

LendTech Operating Models

There are four (4) primary models used by Fintech companies to provide lending products or services in Nigeria.

1. Money Lenders' Model
2. Cooperative Model
3. Banking Model
4. Finance Company Model

While various States in Nigeria regulate the first two models, the last two models are held at the Federal level. Each of these models is further discussed below.

Money Lenders' Model

Money lenders' license is the most widely used license by LendTech companies in Nigeria. This is mainly because the models focused on lending and thus, very easy to operate. There are little to no compliance requirements. Though there is a cap on the interest rate, the cap is nothing that the LendTech company cannot cope with. For instance, the Money Lenders Law of Lagos State caps simple interest rates at 15% for secured loans above N 1,000 (One Thousand Naira) and 12.5% for secured loans of N 1,000 (One Thousand Naira) and below. However, for unsecured loans (which most LendTechs offer), the interest rates could be as high as 48%.

Regulator	Relevant State Ministries, e.g. The Lagos State Ministry of Home Affairs and Tourism.
Primary Legal Regulatory Framework	Money Lenders Laws of various States
Licence	Lenders Licence
Jurisdiction	A money lender may only operate within its State of license; however, they provide their services to persons outside jurisdiction using technology (web and mobile applications).

Cooperative Model

Some Fintech companies adopt the cooperative model because it is easier to operate and offers both savings and lending products - just like banks. However, it should be noted that while a cooperative is allowed to accept deposits from both its registered members and non-members, they are not allowed to lend to non-members. They are also entitled to invest depositor's funds in approved investment schemes and government bonds. This model is unattractive to LendTech companies because it is quite technically challenging to operate due to its accounting and financial models, share capital restrictions, and the cap on interest rates..

Regulator	The Ministry of Cooperatives of various states. E.g. The Lagos State Ministry of Commerce, Industry, and Cooperatives
Primary Legal Regulatory Framework	Cooperative Laws of various States
Licence	Approval to operate a Cooperative Society granted by the Commissioner
Jurisdiction	A cooperative may only operate within its State of a license; however, with the help of technology, they provide their services to members outside their operation jurisdiction.

Banking Model

The Banking model is attractive for businesses looking to offer other FinTech products, including lending. Like a bank, a company can provide lending, savings, and mobile wallet products all rolled into one. Banking models may be classified into two separate categories: the commercial and microfinance banking models. Payment service banks are not allowed to provide lending services. The Central Bank of Nigeria is the regulator for all banking businesses in Nigeria.

Regulator	The Central Bank of Nigeria (CBN)
Primary Legal Regulatory Framework	Prudential Guidelines for Microfinance Banks in Nigeria, the Central Bank of Nigeria Guides to Bank Charges, Relevant CBN Circulars on Bank Lending, and Secured Transactions in Moveable Asset Act.
Licence	Commercial Bank Licence and Microfinance Bank Licence
Jurisdiction or Coverage	This would depend on the nature and scope of the licence. A microfinance bank (MFB) has jurisdictional restrictions and is prohibited from operating or opening branches outside the licence area in some instances. The various categories of Microfinance banking licence are further broken down below:

Categories of Microfinance Banks in Nigeria

There are four (4) categories of MFBs in Nigeria:

a. Tier 1 Unit Microfinance Bank

Tier 1 Unit Microfinance Banks with urban authorisation are allowed to operate in the banked and high-density areas. They may not have more than four (4) branches outside the head office within five (5) contiguous Local Governments Areas, subject to the CBN's approval.

b. Tier 2 Unit Microfinance Bank

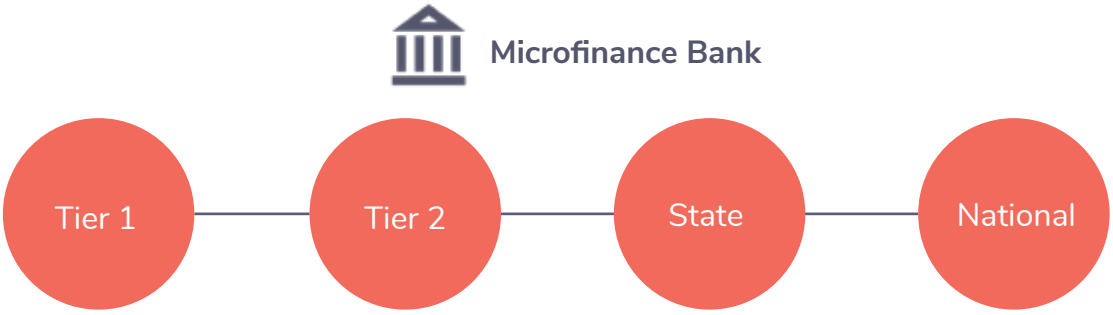
Tier 2 Unit Microfinance Banks with rural authorisation shall operate only in the rural, unbanked or underbanked areas, and are allowed to open one branch outside the head office within the same Local Government Area subject to the approval of the CBN. [14]

c. State Microfinance Bank

State Microfinance Banks are authorised to operate in a State or the Federal Capital Territory (FCT). They are allowed to open branches within the same State or the FCT,subject to the CBN's prior written approval for each new branch or cash centre. However, they are not permitted to open more than two branches in the same Local Government Area (LGA) unless they have established at least one branch or cash centre in every LGA of the State. Note that a newly licensed State MFB is not allowed to commence operations with more than ten (10) branches.

d. National Microfinance Bank

National Microfinance Banks are authorised to operate in more than one State, including the FCT. Note: Newly licensed National MFB cannot commence operations with more than ten (10) branches.



Finance Company Model

As a Finance company, a LendTech company can operate and offer an extensive range of credit products outside lending. Such a company may provide other services such as asset financing, issuance of payment cards and tokens. However, LendTech companies often avoid this model due to the regulatory bottlenecks or what they refer to as "complex" compliance requirements. Besides, the model does not allow them to provide any other services other than credit services.

Regulator	The Central Bank of Nigeria
Primary Legal Regulatory Framework	Revised Guidelines for Finance Companies in Nigeria
Licence	Finance Company Licence
Jurisdiction	A Finance Company may operate throughout Nigeria.

Other Extant Regulations

Some other applicable regulations include:

1. The Nigeria Data Protection Regulation (NDPR) 2019: Although subsidiary legislation, the NDPR is the significant law specifically aimed at addressing data protection in Nigeria. The regulation was issued by the National Information Technology Development Agency (NITDA) in 2019 to regulate personal data processing in Nigeria comprehensively. The law creates rights for data subjects and imposes obligations to ensure security and other safeguards binding on LendTech companies.

2. Federal Competition and Consumer Protection Act 2018: The Act seeks to protect consumer rights in Nigeria. The continuous development and growth of LendTech have made consumer rights very crucial. Without these rights, consumers would be left open to excessive and unfair trade practices, price gouging, market competition, distortion, as well as infringement of their rights.

Section 130 to 133 of the Act protects consumers. These provisions emphasise timely and quality performance and service, delivery of goods free of defects, merchantable products and delivery of products that comply with prescribed standards and practices. The Act provides consumers with rights, including the right to fair dealing [15] and the prohibition of unfair, unreasonable or unjust contract terms. [16] Section 125 prohibits false, misleading and deceptive marketing to consumers. The implication of this is that LendTech platforms cannot make false representations as to the quality of their products or services. Also, the Act mandates service providers to provide information to consumers in plain and understandable language. [17].

3. Cybercrimes (Prevention & Prohibition etc.) Act 2015: The Act criminalises acts committed using online mediums. It imposes an obligation on LendTech companies to take appropriate measures to safeguard users' data. It also promotes cybersecurity and the protection of computer systems and networks, electronic communications (including social media communications), data and computer programs, intellectual property and privacy rights. The Act created several offences that could impact digital lending delivery such as computer-related forgery and fraud, identity theft and impersonation, unlawful access to a computer, breach of confidence by service providers, and phishing among other things. Other laws that regulate LendTechs include the CBN's Consumer Protection Regulation, and the Microfinance Policy Regulation and Supervisory Guideline by the CBN.

LendTechs and Debt Recovery: The Greek Gift

Non-performing loans are a challenge, even for traditional lending institutions. The same challenge confronts LendTechs, with consumers falling into default which racks up the interest rate. LendTechs often have a higher interest rate between 3.5 to 50% annually, which is higher than some traditional banks' loans, contributing to the spike in personal debt. These Apps request from permissions upon installation.

The permission could include the ability to read contacts on a user's mobile phone. Upon default on loan, one of the methods employed towards loan recovery includes calls and SMSs to the contacts on the User's phone. The calls and messages are often framed for the contact to prompt the User to repay the loan. However, we found instances where the messages are communicated in a scandalous and defamatory manner, which misrepresents the relationship's nature or where social media is used to harass users. The constant threat of social embarrassment employed could at best be described as distasteful. The approach bears some semblance with the ingredients of cyber harassment [18] and an infringement of the human person's fundamental rights to dignity. [19] In one instance, a third party whose phone number was on the contact list of a user received a text message from one of the LendTechs that reads as follows:

"THIS IS TO INFORM YOU THAT ****** WITH PHONE NO. ******* IS A CRIMINAL ON THE RUN WITH COMPANY MONEY. WE WILL ENSURE WE MAKE EVERY FINANCIAL INSTITUTION AND ALL ORGANISATION KNOW **** IS A FRAUDSTER. WE WILL GO AS FAR AS TARNISHING **** IMAGE ON ALL SOCIAL MEDIA PLATFORMS. (SHE HAS JUST 2 HOURS TO PAYBACK) THANKS. ******."*** [redacted for privacy reasons]

In another instance, another third party received a message that reads:
"This is to inform the general public that ******* is a chronic debtor on the run with company money. Consequently, It is advised to stay away from **** until **** is arrested."*** [redacted for privacy reasons]

In another instance:
" Please this is to notify the public and all those receiving this messages to disassociate themselves from doing business with ******* AS ****** is a fraudulent individual and on the run with the company's money. You are ****** emergency contact and can be seen as an accomplice."*** [redacted for privacy reasons]

In another attempt:
" Good day, please be informed that ***** took loan from ********** and has refused to pay. We need you to reach **** to pay up ***** loan as the company is taking other unfriendly measures including reporting ***** debt to the Nigerian Police Force as this is a fraudulent act. Note: You are getting this message because ***** gave us your number as emergency contact. you (sic) can as well tell him to remove you if you do not know about this loan."*** [redacted for privacy reasons]

In another instance:
"Goodday (sic), please be informed that ******* has an unresolved financial business with *******. ***** gave your name as an emergency contact should ***** default in the repayment of the loan given to ****. We need you to reach **** and compel **** to pay up **** loan as the company is taking other unfriendly measures including reporting his debt to the EFCC 20 and the Police. **** Legal team"*** [redacted for privacy reasons]

It is essential to point out that the Nigerian court has ruled that both the Police and the EFCC are not debt recovery agents. [21] It is surprising how a default on loan is framed and misrepresented as a crime that has no bearing on the existing relationship between the LendTech and the User. The misrepresentation of facts about a relationship's nature is meant to serve as a social disgrace tool on the User for defaulting.

The recovery model violates the User and third parties' data protection rights who are not privy to the loan arrangement. Their contact merely exists on the User's device. Furthermore, LendTechs in the habit of sending these kinds of messages may have difficulty establishing the appropriate lawful basis for processing third parties' data, not their customers. [22]

According to the CBN's Consumer Protection Regulation, a financial institution is not expected to contact friends, employers, relatives or neighbours of a loan defaulter except they consent to be contacted. [23] These third parties cannot be mandated to offset the financial obligation unless they act as a guarantor to such a loan. [24] Similarly, the CBN's Consumer Protection Guideline on Responsible Business Conduct stipulates that "debt recovery processes are courteous and fair, devoid of undue pressure, intimidation, harassment, humiliation or threat." [25] The art of swinging the pendulum of social disgrace and harassing a loan defaulter's contacts and relatives is not a fair debt collection practice.

There also seems to be a problem with data quality and accuracy - where even after paying up the debt, a User's name may continue to exist on the list of debtors. In one instance, a User of a LendTech interviewed told us:

"I paid back my loan over three weeks, but it was not confirmed. I received calls from about five different people asking me about the same loan. Sadly, they still sent messages to my contacts telling them I still owe them money. "

We also found an instance where it was difficult to repay a loan to one of the providers before the default date, which could be a strategy for the interest to accumulate. According to a User:

"My loan was due, and the App was not accepting my repayment. After about two days, an official from the company sent me a message via SMS containing account details which I was instructed to pay into, which I did. However, by then, the interest has heaped by two-day default. Unfortunately, the App did not acknowledge my payment, and the interest rate keeps increasing daily."

To make matters worse, some providers go as far as reporting customers to the credit bureaus when they have since repaid their loans, putting them at the risk of being blacklisted and denied credit in the future.

It is essential to point out that not all LendTechs use the described model to recover a debt.

According to the CBN's Consumer Protection Regulation, a financial institution is not expected to contact friends, employers, relatives or neighbours of a loan defaulter except they consent to be contacted

Terms of Use: Keep Borrowing or Die Borrowing

Some LendTechs are reputed for concealing their service conditions within insidious and opaque Terms of Use, which are either not placed in conspicuous places for Consumers to read, or made too wordy and rendered incomprehensible to the User contrary to the requirement of the law. [26] ***Our findings revealed that fourteen of the apps reviewed did not prompt Users to read their Terms of Use before signing up.***

According to one of the Terms we reviewed, it stated that ***"to comply with local Know Your Customer (KYC) policy, we may dial someone in your contact list, SMS, call list or other personal information you provide with us."*** A quick review of the Central Bank of Nigeria Revised CBN Anti-Money Laundering/Counter-Terrorism Financing (AML/CFT) Manual, 2009 [27] , revealed no such requirement to pilfer the personal information of users to replace standard KYC procedure was in existence, thus making such acts misleading and false. We have drawn up a list of peculiarly worded clauses from various Terms of Use reviewed, and we provided our alternative meaning:

1. ***"You hereby agree and authorise **** to verify information including, but not limited to, data relating to your phone (including, without limitation, your phone's history, log and location) from your Equipment, from any SMS sent to you or by you, from any 3rd party applications, and such other information as **** shall require for purposes of providing you the Services;"*** (We want to scroll through your phone call log, read your texts and your location history just to get to know you better before giving you this loan of N50,000).
2. ***"In the event that an Event of Default occurs, the Borrower grants to **** the right to notify the Borrower and any other person who, in **** opinion, may assist with the recovery of the outstanding Loan amount and you further agree that this notification may be done by any means of communication which **** deems appropriate;"*** (If you default, we could decide to call your spiritual leader, boss or maybe even your potential spouse; anyone we find interesting).
3. ***"For the purpose of debt collection and without prejudice to this agreement, where the loan is past due (overdue), and concerted efforts have been made to contact the borrower to recover the loan without success, the borrower expressly authorise the Lender and its agents to make reasonable contact with the borrowers Family, Friends, guarantors and workplace for the purpose of recovering the loan;"*** (Basically, we gave the loan to you and your entire family, so they have to get involved since you all now bear the same names).
4. ***"The Borrower authorises **** to disclose any information or documentation relating to the loan to the general public including but not limited to the borrower's employer (where the Borrower is in salaried employment), friends, family members and relatives, professional associations and any other body associated with the borrower in the event that the loan has ceased to be serviced by the Borrower."***

(Loan for you is a loan for all since we discovered that you are one and many, so we have to let everyone know that while you did not commit any offence known to the laws of the Land, we reserve the exclusive right to embarrass and disparage you nonetheless).

These Terms are examples of recurrent clauses found in the Apps we reviewed, and they connote a worrisome trend among LendTechs wherein arbitrary clauses, and terms are hidden in between the fine print of long and wordy Terms of Use. Besides, the law prohibits unfair, unreasonable or unjust contractual terms. [28] A term or condition is considered unfair if it is excessively one-sided, and if the terms of the transaction are adverse to the interests of the consumer. [29]

The law mandates that Terms of Use be simple and easy to understand for the Users as they guide Users to the App's workings and conditions of the service. [30] This is perhaps the main reason why such Terms are kept separate from the Privacy Notice. The practice of bundling Privacy Notice and Terms of Use together fails to implement the data protection principle of transparency at all levels. Our findings have observed that Lendtechs have a penchant for misleading the Users by hiding relevant privacy-invasive clauses in a segment of unrelated items. This practice is contrary to the principle of transparency and irresponsible as it erodes the trust Users have in Lendtechs over time and attracts concerned regulators.

The continued misrepresentation of Terms by LendTechs while it may attract quick returns indicates a lack of adequate regulatory oversight and User awareness on these unethical practices. Users have a right to fair dealing under the law. [31]

Besides, there is a report that one of the Apps used a lesser repayment date than it is required [32] according to Google rules. According to the Rules, "personal loans which require repayment in full in 60 days or less from the date the loan is issued. " [33] However, the LendTech profiled in the report required between 7-30 days, a contravention of the App hosting rules.

Furthermore, it is essential to note that LendTechs Apps, although similar in the model, are different in functionality. Thus, we observed a copy and pasted model of Terms of Use by various Lendtechs which is wrong and impractical. Each App should have its different Terms of Use as they were likely created separately with distinctive features.

The continued use of templated Terms of Use not fit for their specific context is a clear misrepresentation of service and the conditions of using such an App by Users. The law prohibits the making of false, misleading or deceptive representations. [34]

- In the event that an Event of Default occurs, the Borrower grants to ..... the right to notify the Borrower and any other person who, in ..... opinion, may assist with the recovery of the outstanding Loan amount and you further agree that this notification may be done by any means of communication which ..... deems appropriate

- "****** is not an organization registered with the Reserve Bank of Nigeria and does not hold any license to engage in any activities relating to lending or borrowing. ******* is not a Financial institution under the Companies Act 2013 or the Banking Regulations Act, 1949 or any other laws for the time being in force in Nigeria"

- "You further understand that ****** is not a Financial Institution under Companies Act 2013 or the Banking Regulations Act, 1949 or any other laws for the time being in force in India. ****** is also not a deposit taking company or a chit fund or a company offering any investment schemes as per the rules and regulations for the time being in force in India"

The law mandates that Terms of Use be simple and easy to understand for the Users as they guide Users to the App's workings and conditions of the service

LendTechs and Data Protection

Data protection is concerned with safeguarding personal data from abuse, misuse, unauthorised access, and security of the data subject's rights. Because the credit bureaus cannot provide on-the-spot credit score of borrowers, some LendTechs use personal data obtained from the borrower's smartphones and social media platforms to determine the borrower's creditworthiness. Also, some lenders access the borrower's contact list and social media friends list (this is possible where the borrower signed up using a social media platform) to contact them when the borrower defaults. The privacy notices of some the LendTech do not state the purpose of collecting the large volume of data they demand. The obligation to ensure data protection is both a statutory requirement and App hosting policy. [35]

Our findings revealed that some of the LendTechs violate the data protection rights of the data subjects, fail to implement the principles of data protection, are low on transparency, sends unsolicited and marketing correspondence to non-users as a customer acquisition strategy, [36] use excessive permissions and trackers without obtaining the consent of users or notifying them about its existence, adopt poor security design, grant third-party access and data requests, and share data with third parties (including advertisers).

Excessive personal data collection is contrary to the principle of data minimisation, which requires that personal data should not be processed for more than what is necessary. Listening to a user's phone call, reading their SMS, harassing their contacts who are not privy to the loan is a gross violation of extant data protection laws. Similarly, installing trackers capable of profiling users and sharing personal data with third parties without obtaining user consent is a violation of the law. Unfortunately, the third parties with whom the data are shared have a long list of other third parties they share the data with. [37] There is a report about one of the Apps that scans a User's contact "to see if they include a known debtor". [38 . 39] Unfortunately, none of the Apps reviewed drew the attention of Users to the existence of trackers embedded in the App, let alone allow them to consent to it.

Users are mostly unaware of the divergent data-sharing practices that exist between companies. There is no method to opt-in (or opt-out) of third party tracking or notifying users of its existence within the Apps' architecture. This means any personal data such as unique identifiers (e.g. your phone's Advertising ID) could be sent to third parties without the appropriate lawful basis, which is a breach of the Nigeria Data Protection Regulation (NDPR) and other extant laws.

To put this in context, one of the privacy notices we reviewed stated that:

" you have the right to stop our access to your personal data. Should you wish to stop sharing information, you can uninstall the * App."***

In another instance, it reads:

"you can withdraw your consent to our collection, processing or use of this information at any time by logging out and uninstalling the App from your Device."

Uninstalling an app is not the same as deletion or erasure of such data. In other words, uninstalling an application does not give users the control and rights guaranteed under the law. Such data continues to be retained by LendTech.

"By Downloading and Using any of our services, you consent to our automatic collection of data relating to your location via GPS Technology or other location services."

This is contrary to the requirement that consent should be specific. There is no explicit disclosure about the retention of data.

Another issue of concern is around the international transfer of data. Though there are no rules around data residency, data shared through third-party requests on websites and third-party trackers on the mobile App are moving to countries outside Nigeria. There is no evidence of complying with the rules, as the privacy notices primarily did not address the international transfer of data. The failure to address international data transfer could leave Users unprotected and without relief if such data is transferred to countries without a data protection law or an adequate law. [40] It is questionable as there are reports that data are moved to countries that are not considered sufficient human rights protection. [41] [42]

A member of the research team that received unsolicited texts from two providers made a data subject access request and never received a response in two instances, outside the statutory one-month duration [43] - which may establish they do not have measures to enforce and comply with data subject rights requests.

None of them provided a straightforward way to opt-out of the services. The Apps that had trackers in them lacked a mechanism to opt-in and opt-out of third-party tracking.

Review of Privacy Notices

The User's (data subject's) right to be informed [44] and the transparency obligation on data controllers (LendTechs) is a crucial data protection element. A privacy notice is a public-facing document from an organisation that explains how it processes personal data and applies data protection principles. The NDPR requires entities to make their privacy notice available comprehensively and readily accessible to the data subjects. [45] Statutorily, a privacy notice is expected to be placed in a conspicuous place for the User to read. According to Google Developer Policy, the privacy notice is expected to "disclose the types of personal and sensitive data your app accesses, collects, uses, and shares and the types of parties with which any personal or sensitive user data is shared". [46]

Our findings revealed varying levels of compliance with this obligation. Whilst only four of the Apps had no privacy notice, the rest had a privacy notice that either failed to comply with the regulatory requirements; [47] or lacked sufficient details or could not address the mobile application's processing. Some privacy notices were incomplete or vague.

In many cases, the privacy notices were drafted like a contract or bundled into the terms of use. The notices also failed to give sufficient information on the use of cookies, [48] tracking technologies, third-party requests, inability to notify the data subject about their rights or had no contact information provided that Users can reach out in the event of a complaint. Some of the notices were evasive about the type of information collected on the mobile application. Besides, there is no sufficient information on the use of trackers and adverts or the option to opt-out of adverts (for those that embedded adverts into their mobile application).

- **In one instance, the email address provided as contact information was incomplete. In some of the notices, we found the use of severability, arbitration and limitation of liability clauses or citing of non-Nigerian law.**
- **68 % of the mobile applications did not have their notice conspicuously visible to the Users.**
- **In one instance, the App belongs to one of the commercial banks with no prompt for permission, no link to their privacy notice inside the App or on the Playstore.**

68% of the mobile applications did not have their notice conspicuously visible to the Users.

Summary of the privacy notices concerns is summed up below:

None had their privacy notice specifying the lawful basis for processing personal data;

- 50 % had their privacy notices drafted like a contract;
- 18 % did not have a privacy notice;
- 40 % had incomplete privacy notice;
- Two had privacy notices not designed for Nigerian users, citing the United States and Kenyan laws;
- Two did not have complete contact information;
- 40 % did not mention the rights available to the data subjects;
- One of the notices led to the terms of use; and
- None had a transparent cookie notice nor addressed the permissions or trackers on the mobile App.

Review of Websites

Some of the apps have functioning websites, majorly for general information purposes only. The website also hosts their privacy notices.

Summary of the concerns with the website are stated below:

- 36 % of the websites had no Secure Socket Layer (SSL).
- 68 % of the websites had no Content Security Policy (CSP) enforced.
- 68 % of the website had no Referrer Policy.
- 22 % of the website had their cookies transmitted via an unsecured channel.

Use of tracking technologies: Keeping up with my Debtor

Tracking exists on both website and mobile application. Tracking is profiling which is “any fully or partly automated processing of personal data to evaluate personal aspects of a natural person. Tracking could be first-party (if the app owner owns it) or the third party. [49] Tracking provides the App owner with the capability to uniquely identify or track users’ behaviour across multiple digital services. [50] Besides, when these data are combined with other apps, online browsing history and behaviour can generate individuals’ very detailed profiles. [51] “The extent of tracking makes it impossible for us to make informed choices about how our personal data is collected, shared and used.” [52] Furthermore, “the widespread tracking also has the potential to seriously degrade consumer trust in digital services.” [53] Limiting third parties’ tracking capability on mobile application is near absent compared to web browsers, which allows the use of third-party plugins [54] and default browser settings. [55]

According to Google Protection Levels, apps flagged as dangerous require the consent of the User. [56] Trackers meant for advertisement assist the App owner in generating revenue by monetisation of the behaviorally targeted advertising. Monetising Users behaviour could have an impact on Users without their knowledge. It is even more dangerous because none of the LendTechs using these Ads trackers made reference to it in their privacy notice or allowed Users to consent to it or opt-out of it lawfully. Some of these risks include targeting vulnerable populations, minority groups, or those in financial difficulty, resulting in differential pricing or depriving certain groups of opportunities. [57]

Our findings revealed extensive use of third parties' trackers. 68 % of the mobile applications analysed had third party trackers embedded in them, which included behavioural profiling to advertisers and social media platforms. In some instances, the advertisers also share data with other third parties. [58]

Our findings established that some of the Apps used intrusive permission flagged as dangerous by Google Protection Levels and did not get the User's agreement before installation. The permission ranged from the permission to read and receive SMS, read phone state, read and write calendar, calling phone, write and read external storage, access media location, and record audio.

According to Google Protection Levels, "Only dangerous permissions require user agreement." [59] The Google PlayStore requires Apps to ask for permissions in context when the User starts to interact with the feature that needs it. This is similar to the statutory requirement that consent should be specific. "Dangerous permissions cover the areas where the app requests data or access to resources that involve private user information, and could potentially affect the personal data stored on the User's device." [60] [61]

According to Google Developer Policy, [62] the App developer must provide an in-app disclosure. The disclosure is expected to be displayed in the regular usage of the App and not require the User to navigate into a menu or settings before it can be accessed. Disclosures should also describe the data collected and how the data will be used and/or shared. The "in-app disclosure must accompany and immediately precede a request for user consent and, where available, associated runtime permission". [63] Consent (when it is the appropriate lawful basis) should not be obtained from the User through force or manipulation. Instead, App developers should accommodate all users and respect their decisions if they decline a request for permission. [64]

68% of the mobile applications analysed had third party trackers embedded in them

Indeed, a good number of the LendTech have complied with these requirements in disobedience. The excessive use of permissions and trackers is a violation of the data minimisation principle. Data collected should be limited to what is necessary for the application to provide the service. Similarly, the failure to explain the purpose of the data processing on mobile apps is a violation of the data protection principle of transparency, which requires controllers to inform users about their processing activities. The obligation to provide a privacy notice is both a requirement of the law and App hosting (Google Playstore).

Summary of Permissions considered dangerous by Google protection levels used on mobile applications:

- 64 % of the apps are capable of reading phone state;
- 32 % of the mobile applications can read the calendar on the phone, and 18 % of the apps can write on the phone's calendar and its data;
- 18 % of the mobile applications can answer and place calls, and fourteen apps can access or modify the phone state;
- 81 % of the mobile applications can access external storage (e.g. SD card) in a write or read mode;
- 64 % of the mobile applications can read or write a phone's contacts;
- 36 % of the mobile applications can read SMS, and 14 % is capable of receiving SMS;
- 9 % of the mobile applications record audio on the mobile phone;
- 64 % of the mobile applications have access to the geographical location of the media content of the mobile phone;
- 50 % of mobile applications can use the camera for taking pictures or record videos; and
- 55 % of mobile applications have access to the geographical location of the mobile phone.

LendTechs and Cybersecurity

Stewart Room once said, **"if data protection principles are the celebrities of the data protection world, security is always on the A-list, a true VIP"**. This notion is based on the fact that, unless personal data is protected against malicious or accidental unauthorised access (confidentiality) or modification (integrity) by securing it, then privacy may be impacted.

The security principles of confidentiality and integrity are also principles under data protection, which mandates organisations (LendTech inclusive) to implement technical and organisational measures. [65] Consequently, LendTechs are expected to ensure they provide adequate security on both the mobile application and website to avoid a security incident or a cyber attack which may inadvertently or maliciously lead to a data breach. We carried out a security assessment of ten (10) LendTech mobile applications (apps). This assessment's scope is limited to apps with the Android Operating System (OS) using open-source standard testing guides. The area of this assessment is limited and does not consider mobile applications in a dynamic environment.

The summary of the findings from the mobile application security assessment is stated below:

- 20% of the mobile application contains potentially sensitive hardcoded data. 40% of the apps also have code that enables communication in clear-text. An attacker with access to the mobile application file can easily extract either of these data from the application and use it in further attacks.
- 60% of mobile applications reviewed use the unencrypted HTTP protocol. These mobile applications use the HTTP protocol to send or receive data. [66] The HTTP protocol design does not provide any encryption of the transmitted data. This increases the impact when such traffic is intercepted if an attacker is located in the same network or has access to the victim's data channel. [67] The HTTPS protocol allows for the encryption of data in transit.
- Within the context of protecting data at rest or in motion, encryption is one of the most acceptable means of achieving such protection. A poorly implemented encryption algorithm may be as bad as having no encryption - providing a false sense of security. 60% of the apps reviewed have weak or poorly implemented encryption algorithms, which can endanger the mobile application's data storage and transmission;
- Also, 20% of the mobile applications use Predictable Random Number Generator. Under certain conditions, this weakness may jeopardise mobile application data encryption or other protection based on randomisation. For example, suppose encryption tokens are generated inside of the application. In that case, an attacker can provide an application with a predictable token to validate and then execute a sensitive activity within the

application or its backend; and injection vulnerability in the mobile application. The correct approach is to use prepared SQL statements beyond the User's control. [68]

- 10% of the mobile application uses external data in Raw SQL Queries. The inclusion of input into raw SQL queries can potentially lead to a local SQL injection vulnerability in the mobile application. The correct approach is to use prepared SQL statements beyond the User's control.

The importance of security in such mobile apps cannot be overstated. This is because of the scale and magnitude of its impact. In most cases, security issues scale beyond individual users to majorly all users of the applications which may number in thousands or more. Therefore, it is essential that, just like privacy, security is built-in rather than bolted-on the mobile applications from the initiation phase of requirements gathering, solution conceptualisation, and design until the public release.

LendTechs and Consumer Protection

Digital lending is easy and quick, and borrowers are susceptible to aggressive marketing, fraud, misrepresentation, compelling marketing strategies like unsolicited loan offers, and misrepresentation of terms, which encourage borrowers to take loans without adequately considering the need to repay it. While some misrepresent, some others may fail to display interest rate and pricing. Google Play Developer Policy requires apps offering personal loans to disclose critical information such as the minimum and maximum periods of repayment, the maximum annual percentage rate, a representative example of the total loan cost including all applicable fees, and a privacy notice that comprehensively discloses the access, collection, use and sharing of personal and sensitive user data. [69] Besides, lenders licensed under Money Lenders Laws of various states are not so regulated. They enjoy some freedom, giving them a competitive advantage over other lenders who are much more strictly regulated. This practice, in a way, eliminates fair competition among the money lenders.

The use of skewed terms of use creates an asymmetrical relationship and imbalance in rights and obligations against the User's interest is considered an unfair practice and prohibited under the law. [70]

There is also a concern that some credit scoring algorithms that use data like educational or literacy levels or past debtors' existence on phone contact may unintentionally lead to discriminatory lending practices. Lenders partner with the credit bureau and send the name of loan defaulters to the latter for record of creditworthiness.

As previously highlighted, one of the biggest complaints from Users is that some of the loan lending platforms charge arbitrary interest rates on loans, with repayment spread over a long tenure. Another unfortunate aspect is the ambiguity and opaqueness of terms of use and how the interest rates are calculated, trapping consumers in a cycle of indebtedness. Some of the lending platforms have devised vague computing interest rates for users, thereby unjustifiably increasing the repayment tenure to ensure users pay more. [71]

Interestingly, both the Federal Competition and Consumer Protection Act and the CBN's Consumer Protection Regulation have explicit provisions and obligations to provide sufficient information to users about service quality and prohibit unfair contractual terms. [72]

LendTechs and Dark Pattern: Manipulation by Design

Dark Patterns are tricks used on websites and apps that prompt consumers to do things that they did not mean to, like signing up for something. [73] It is a misleading or otherwise deceptive user interface or user experience decision that tries to exploit human psychology to get users to do things they do not want to do. [74] From nudging a consumer to provide more information than they should, to positive reviews in favour of a product, to being used to deceptively obtain consent or manipulating consumers to decide in favour of a service provider. Dark patterns manifest in variegated ways.

Our research found the use of dark patterns in some of the mobile applications. We found social proof to influence Users' behaviour by describing other users' experiences and behaviour. [75] **Five of the apps reviewed had positive reviews that are targeted to sway the decision of the Users.** However, the comments appeared not to emanate from the Apps users, but rather a positive review as-a-service. [76] The reviews used a non-Nigerian currency about the loan it got on the App. [77]

We also found obstruction, making it easy to sign up for the mobile application's service but difficult to stop using it or opt-out. **In two instances, the mobile application's terms of use specified that Users could opt-out by uninstalling the mobile application** and omitting to identify what will happen to the Users' existing personal data retained. The Users interviewed provided insight into how it is easy to sign up on the apps, but how complicated it is to delete them. Unfortunately, none of the Apps reviewed has a clear information on how to opt-out of the service.

"The deception enabled by dark pattern design not only erodes privacy but has the chilling effect of putting web users under pervasive, covert surveillance, it also risks enabling damaging discrimination at scale. Because non-transparent decisions made off of the back of inferences gleaned from data taken without people's consent can mean that — for example — only certain types of people are shown certain types of offers and prices, while others are not." [78] Beyond the privacy implication, digital nudging to manipulate consumers' decisions favouring a business is a classic case of human behavioural psychology's commodification. While there is a valid case for a legitimate marketing strategy for a company, crossing the line of ethics and legal regulation is an anomaly. Designers and business may contemplate the manipulation matrix for ethical behavioural design consideration. [79]

★★★★★ 11/15/20

Nigeria loan app always comes through! The app is super easy to navigater. Small amounts but helps when tight. You don't get stuck paying high interest fees or hundred of dollars back. I have referred nigeria loan app to a few friends now. It would be nice if they offered some type of incentive to refer people to nigeroa loan app., but either way it's a good service

★★★★★ 11/15/20

The nigeria loan app has really pulled thru for me when i truly needed it. Overdrafts can get really expensive very fast. Knowing that nigeria loan app has my back by helping me with $75 to help prevent overdrafts is such a relief! I don't always need help preventing overdrafts but when they do come about, having nigeria loan app there to save my &#$ is such a relief!

★★★★★ 11/21/20

I honestly thought this was just another app to try to make you pay some outrageous amounts, just to get your spending habit in order. I was VERY wrong! Of course i'm only 20 and it's terrible to say i was one of the millennials who spent thousands on unnecessary items. loan app helped me budget and when i neeede it spot me up to $75! Now i barely use the cash advances becasue i've learned how to spend wisely

★★★★★ 11/13/20

Within the last year or two things were pretty tight financially, so i looked into apps like this to help me out. I literally downloaded over 30 apps and signed up for every single one. 1. Minimum wage amounts (some as high as $10,000 a month). 2. Evidence of Direct Deposit (thise excludes bank to bank transfers, and transfers from self-employment businesses such as DoorDash) 3. Hour tracking (this means your workplace either has to be a partner with the app OR you have to use GPS tracking so the app can physically detect when you go to and from work, one location only. Not only did I not make enough to qualify for most of the apps with high minimums, but my workplace didn't offer direct deposit, AND i worked for a business with multiple locations so i would only be getting hours for one location which was maybe a third of my total hours. I ended up with only two apps that i could actually use.

★★★★★ 11/23/20

In times like these, it's great to use this app to help make ends meet. I have only use it a couple of times, but it has truly helped me when times are tight. I like that the money is automatically pulled out my account on pay day and i don't accure daily or high interest fees on payback, i'm so glad i found this service. it's much better than payday lenders that charge outrageous rates

Use of Artificial Intelligence (AI) by LendTechs

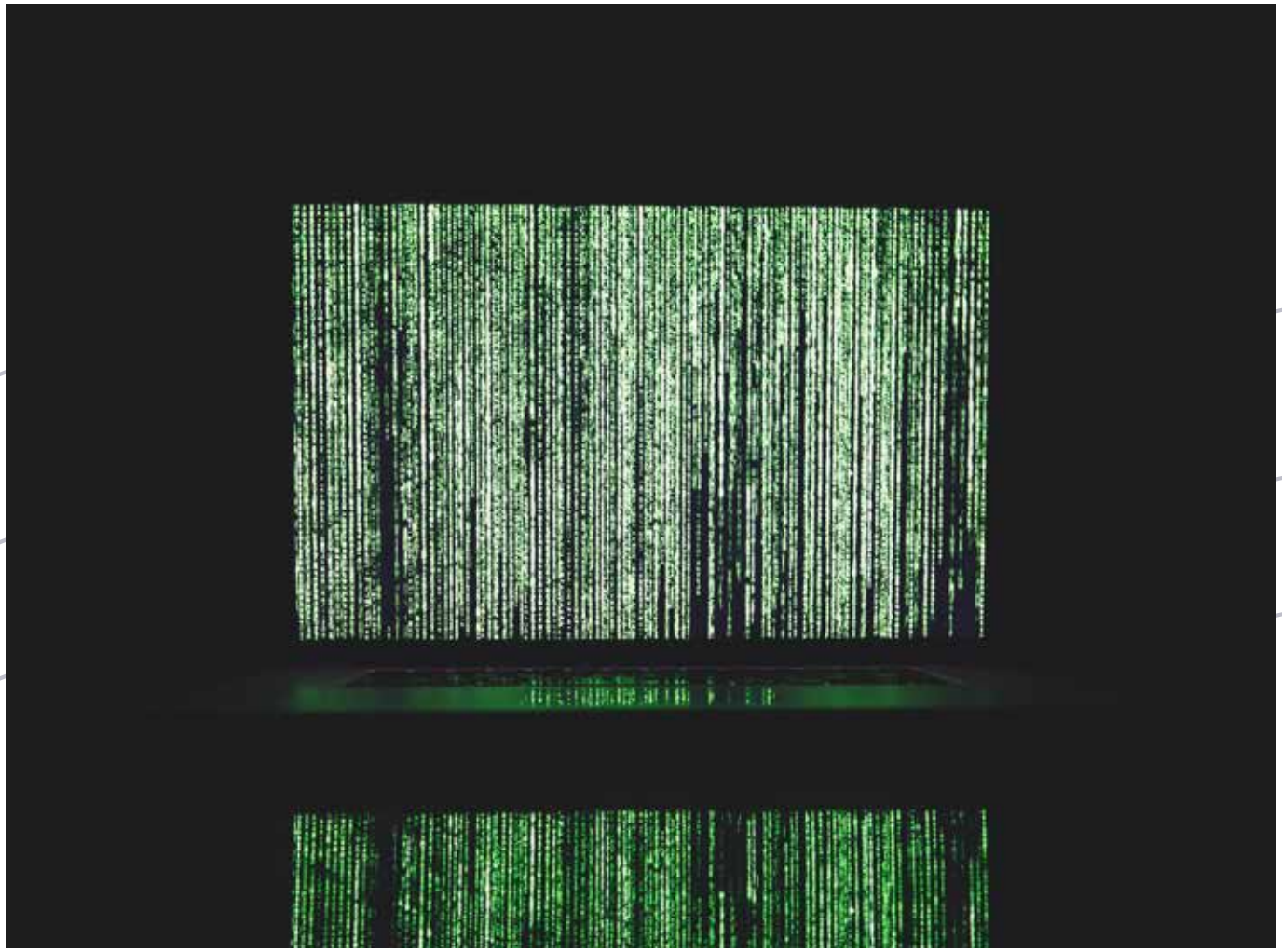
It is a fact that Artificial Intelligence (AI) is increasingly being used in various sectors. It is, therefore, not surprising that banks and LendTechs are also adopting AI. Data is an integral part of money lending, and AI serves as an invaluable tool in this regard. Generally, the more data available to the money lending firm, the easier it is to determine the borrower's creditworthiness. Studies reveal that AI and ML's incorporation improves credit markets' efficiency and accuracy by assessing their borrowers' creditworthiness. [80] With these technological innovations, credit risks can be evaluated from the borrower's financial data and by considering alternative data - from the borrower's digital footprints, including social media use, internet browsing, geolocation data, search history, purchase history, among others. The AI and ML algorithm uses the assessed data to provide credible insight or credit scores that can be utilised to predict the borrower's likelihood of defaulting on the loan repayment. One of the LendTech websites states it uses AI for creditworthiness assessment, which significantly reduces its loan default.

As the adoption of technological innovations in predicting credit scores becomes widespread, there is a rising concern about the risks inherent in using AI and ML to assess high quantities of data continuously. First, there is the challenge of AI or ML bias; the models integrate the bias reflected in the data used in their training. [81] The prediction power of AI depends on the data it is inputted with; since humans produce the data, the dataset often carries all the human bias. In the United States of America, for instance, increased ML bias has been used to discriminate against black people and other minority ethnic groups such that their credit scores do not reveal their accurate creditworthiness, resulting in a disproportionately high number of black people receiving rejections on money lending applications in comparison with white borrowers. [82] Availability of accessible data might be a way of reducing the incidence of ML or AI bias.

We found 32 % of the LendTechs using machine learning and/or artificial intelligence for their proprietary credit scoring and credit risk assessment algorithm, which decides on a User's suitability for a loan or otherwise. [83] **However, only one (1) provided information in its privacy notice about its existence contrary to the requirement of the law.** 84 Unfortunately, the NDPR does not have the right not to be subject to a decision solely based on automated processing which produces legal effects concerning the data subjects specifically recognised, which would have conferred the data subjects the right to demand an explanation for the automated decision and challenge it. Furthermore, AI-driven algorithms might generate outputs which have a discriminatory impact on some classes of people. This means borrowers might be discriminated against, and denied credit based on the data assessed by the algorithm.

The privacy concern arises from digital lending firms having access to various data -sensitive data inclusive. The massive collection of data used by AI simplifies privacy invasions [85] - with most data collected without the borrowers' knowledge or any other appropriate lawful basis. Further to this is an ethical concern regarding the use to which the data is put or the type of data used in determining creditworthiness. Moreso, data breach possibilities also heighten security concerns, considering the amount of data involved.

Also, the black-box effect, which refers to the inability to give plausible explanations on AI's decision-making process, raises issues around the lack of transparency and non-verifiability of AI algorithms' results. To this extent, appropriate safeguards must be implemented using Machine Learning and Artificial Intelligence in the digital lending sector.



Recommendations: Navigating the Murky Water

Privacy and Data Protection

They should consider less intrusive and privacy-preserving models for their application and websites, which will process fewer data or strictly necessary data to provide services in compliance with the data minimisation principle. Their privacy notices should genuinely reflect their processing activities and should also be made available in an understandable format, language, and conspicuously to see it. The privacy notice should address the mobile application's specific processing on the web, including permissions, trackers and third-party requests.

They should ensure they have the appropriate lawful basis before commencing processing activities. For example, where consent is required for permissions, they should validly obtain it. They should avoid bundling privacy notices with terms of use, they are two distincts documents with different purposes. Both the terms of use and privacy notice should be written in an easy to comprehend manner. Also, attention should be paid to the international transfer of data, and they should ensure they have the appropriate basis to transfer data outside Nigeria. They should ensure that the third country has an adequacy decision from NITDA or that such transfer should be made under any of the derogations. [86] They should conduct a scoping and mapping their processing activities to understand their data life cycle management better. They should document their processing activities in a record of processing activities, which would assist with accountability and demonstrate compliance with the law.

LendTechs should improve on accountability by implementing data protection by design and default into the design methodology for technology and other relevant processes. For LendTechs using Artificial Intelligence (AI) or Machine Learning (ML) to profile and determine credit worthiness, a Data Protection Impact Assessment (DPIA) should be conducted before deploying the solution because of the high-risk nature of the processing activities. A DPIA is a necessary statutory requirement where automated processing with legal and significant effect [87] and processing involves sensitive personal data. [88] The DPIA should either be made available publicly or on request. The algorithm dataset and quality should be audited to prevent bias or discrimination by shutting out people who deserve credit. Algorithms should be reviewed from time to time to see whether they introduce unwanted discrimination.

They should consider appointing a data protection officer (DPO) to ensure compliance with the data protection law. [89] The DPO can assist them with developing and implementing a privacy program, including data subject rights. They need a mechanism and procedure to address data subject rights and complaints. They should conduct a third-party

audit or assessment to give them a clear picture of where they stand and possible areas of improvement; the audit should be performed periodically. They should consider adopting privacy-preserving measures and tools.

Security

LendTechs should improve the security on both apps and websites to safeguard the consumer. There are reports of fraud and other cybercrimes done through these services. They should consider security from the design stage and continuously improve it by periodic updates and patching of vulnerabilities. The various platforms involved should ensure that Security by Design (SbD) is implemented. At a minimum, mobile security assessment should be conducted before the public's mobile apps' roll-out for use. Regular Vulnerability Assessment and Penetration Testing should be performed periodically to improve security posture.

Dark Pattern

Though the Nigerian law does not expressly prohibit the use of dark patterns, the semblance of relief lies under the data protection and consumer protection framework to protect Users from deception and manipulative behaviour. Besides, Google disallows deceptive conduct on its Playstore. [vv] Mobile apps and websites should be designed in ways where dark designs are not used to manipulate users into making a predetermined decision favouring the LendTechs.

Terms of Use

The terms of use should be more transparent and clear on the metric for computing the interest rates or specify the rates. LendTechs need to present prices, conditions, and conditions clearly on the digital interface. The digital lender's identity should be ascertainable; non-provision of contact information is deceptive and evasive. Terms of use should genuinely reflect the nature of a relationship and should avoid unfair terms or misrepresentation of nature of service.

Regulation and Governance

Through the Central Bank of Nigeria (CBN), the government should consider creating a regulatory landscape to provide oversight in the industry, especially in service delivery, data protection, technical and organisational security, accountability, and governance. There is a need to define a threshold for interest rates to prevent arbitrariness and unscrupulous default. LendTechs lack supervision against fraud, terrorism financing, and money laundering, which are matters of prudential financial regulation, within the financial sector regulator's powers, like the CBN.

LendTechs partners with third-party operators who collect, analyse, and process customer data. They mostly fall outside of the supervision of financial regulators. There is the need for the CBN to include LendTechs under the digital financial service providers as was done by the Central Bank of Kenya (CBK) through an amendment of the Central Bank Act. The CBK defined digital financial products and services and put them under its regulatory power. It recognises digital credit. This will allow for fair competition and proper consumer protection.

LendTech needs to have complaint resolution mechanisms. Complaint Resolution systems need to be available to consumers, preferably including speaking directly to a person. Lenders are advised to inform customers frequently about how to resolve problems.

From an ethical and best practices point of view, LendTechs should consider self-regulation by reviewing the categories of persons who can access loans, minimum age requirement; income and other relevant information could be a criterion, which reduces the chances of default of vulnerable populations pulled into the debt cycle. [91] LendTechs, especially those not regulated by the CBN might have a thing to learn from the Apex bank's direction on responsible lending. [92] These may include reviewing credit history, improving credit risk assessment procedure, assessing capability to repay sustainably, and monitoring loan performance.

The FCCPC should exercise its regulatory oversight in consumers' interest in misrepresenting the quality of services, unfair contractual terms, and fraud. Besides, the Commission is empowered to exercise concurrent jurisdiction with other regulators. [93] Consequently, the FCCPC should take steps against operators who act contrary to the representations made in their terms of use and privacy notice [94] , offering services with unfair terms of service and whose practices violate fair dealings. FCCPC should consider issuing a Regulation or Guideline on fair practice in debt recovery to complement the existing CBN framework, significantly because not all LendTechs fall under the CBN's regulatory oversight. The instrument should prohibit the harassment, oppression, abuse, or violation of the User's right to dignity, using the threat to harm their person or reputation.

Further, it should prohibit the use of obscene or profane language, threat to make a report or harass with agents of the State, misrepresent the nature of the of the relationship by falsely alleging commission of a crime, misleading information on the amount or legal status of a debt, implying that non-payment of a debt will result in arrest or imprisonment, and repeatedly calling with intent to annoy, abuse or harass the User or third parties to recover the debt. [95] The data protection authority (or any government agency exercising such power) and the Federal Competition and Consumer Protection Commission should enforce the general laws to protect Users from these risks. The National Assembly should also speed up work with the Electronic Transaction Bill passage, which would extend protection available to consumers. [96]

Self-Regulation by Platforms

While it appears the regulators should be responsible for regulating the pervasive activities of the LendTechs, a sizable responsibility lies on the shoulders of the different app stores hosting these applications. They have sweeping powers to rein in strict rules and demand standards that are privacy and consumer-centric. In January 2021, Google announced it removed some loan applications from its Playstore in the Indian market [98] and removed another 600 applications for inappropriate Ads placement. [99] For a mobile application to be listed on an App Store, the developers must comply with the App Store owner's policies. Are these policies being enforced consistently? For context, four of the apps we reviewed did not have a privacy notice . An app below the policy standards should be removed. Recently, Apple tightened its App hosting rules by demanding more transparency to host Apps on its App Store. [100]

They should enforce their self-regulation by disabling apps with excessive permissions, misrepresentation, dark patterns and deception, and low transparency. While it is essential to reining in adherence to protect users from some actors' malicious behaviours, it is equally necessary that the policies are enforced consistently to avoid creating a hostile environment for innovation.

User Awareness

Businesses and individuals need to be sensitised on the need for data to help the credit bureaus build their databases. Illiteracy is a problem for some users. Some borrowers are unable to understand privacy notices, terms and conditions and contracts. Many of these platforms use the internet and USSD, how many illiterates can operate them? They should consider the use of quick and short digital surveys to offer simple ways to verify borrower's understanding. Oral tools may be used to pass messages in the simplest form. Privacy notices should be presented in a layered approach and written in an easy to understand manner. The privacy notices and terms of use should be available conspicuously in the mobile application and presented to Users before creating their accounts.

Users should read privacy notices. Notices provide insight into the nature and extent of data processing by an organisation, the data subjects' rights, and how to exercise these rights. Albeit, reading a notice is insufficient, if the privacy notice is not transparent enough or genuinely reflects the processing's nature.

Users should modify privacy settings on their device. It is possible to restrain some of the permission by adjusting the phone settings and the App settings to improve privacy and security. Some Applications collect excessive permissions that are not relevant for them to function effectively. Excessive permissions could result in risks to the data subject. [101] Users should consider disabling unnecessary permissions through the phone setting. This offers users a bit of control.

Users should avoid providing too much data. Users should give only the data necessary for the application' to function. Organisations should abide by the data minimisation principle by using only the data required to provide the services effectively.

Conclusion

This research has proved that there is still much to be done by LendTechs in terms of data protection, privacy, security and consumer protection. LendTechs address a critical problem in our society and are quite essential for accessing micro-credit. However, they must do so responsibly and within the bounds of law, ethics and in consideration of the consumers' interest. Current practices are vulnerable to the violation of data protection, privacy, consumer protection laws or any other extant laws. It is simply not enough to make vague representations of the intention to ensure consumers' interest; it must be seen to be done.

Appendix

What is a tracker?

A tracker is a piece of software whose task is to gather information on the person using the application, [102] how they use it, or the smartphone being used. Trackers could be used for crash reporting, profiling, monitoring location, targeting a user with adverts, analytics and identification

What are permissions?

Permissions are actions the application can do on the phone. An app requires permission to function. Android apps must request permission to access sensitive user data (such as camera, location, and read SMS). [103] A central design point of the Android security architecture is that no app, by default, has permission to perform any operations that would adversely impact other apps, the operating system, or the User. [104] An App must publicise the permissions it requires. [105] Standard permissions do not pose much risk to the User's privacy or the device's operation; the system automatically grants those permissions to your App. Dangerous permissions could potentially affect the User's privacy or the device's regular operation. [106]

What is a referrer policy?

The referrer header allows websites and services to track users across the web and learn about their browsing habits (possibly private, sensitive information), particularly when combined with cookies. [107] By setting a Referrer-Policy, websites can tell browsers not to leak referrers. It helps preserve data minimisation principles. (Article 2.1 (b) of the NDPR)

What is a Secure Socket Layer?

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client (e.g., Outlook). [108] [109] SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. 110 Typically, data sent between browsers and web servers is sent in plain text—leaving the data vulnerable to eavesdropping. If an attacker can intercept all data being sent between a browser and a web server, they can see and use that information. [111]

What is a content security policy?

Content Security Policy (CSP) is an added security layer that helps detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. [112] These attacks are used for everything from data theft [113] and site defacement to the distribution of malware. A primary goal of CSP is to mitigate and report XSS attacks. [114] It helps prevent unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (Article 2.1 (d) of the NDPR).

References

1 Analysing applications in a static state has its limitations and ability to interpret the data payloads, we cannot confirm precisely what data is sent.
2 There were micro-credits granted by microfinance banks and microfinance institutions. There are also co-operatives and other friendly societies that granted micro-loans to consumers. However, these existing systems failed to provide quick access to credit facilities and were not readily open to people. Only a class of people had access to these facilities.
3 Why Are Interest Rates in Nigeria so High?' (28 January 2019) </article/why-are-interest-rates-in-nigeria-so-high> accessed 27 January 2021.
4 Some of the Lenders are able to provide loans as quick as five minutes.
5 'In Search of Quick Loans, Nigerians Give up Privacy' (TechCabal , 14 October 2019) <https://techcabal.com/2019/10/14/in-search-of-quick-loans-nigerians-give-up-privacy/> accessed 27 January 2021.
6 'This Lending App Loves You until You're Late on a Payment. Then the Shaming Begins.' (Rest of World , 26 May 2020) <https://restofworld.org/2020/okash-microlending-public-shaming/> accessed 27 January 2021.
7 'In Search of Quick Loans, Nigerians Give up Privacy' (TechCabal , 14 October 2019) <https://techcabal.com/2019/10/14/in-search-of-quick-loans-nigerians-give-up-privacy/> accessed 27 January 2021. 8 "Murang'a Man Hangs Self over Sh3,000 Mobile App Loan" (Nation, June 29, 2020) <https://nation.africa/kenya/counties/muranga/murang-a-man-hangs-self-over-sh3-000-mobile-app-loan-177764> accessed August 31, 2020.
9 TNN / Updated: Dec 23, 2020 and 13:17 Ist, 'Loan Apps News: Loan Apps Pushing People into Debt Traps, Suicides | India Business News - Times of India' (The Times of India) <https://timesofindia.indiatimes.com/business/india-business/loan-apps-pushing-people-into-debt-traps-suicides/articleshow/79895297.cms> accessed 27 January 2021.
10 'Made in China: How the Instant Loan App Racket Boomed in India' (The News Minute , 12 January 2021) <https://www.thenewsminute.com/article/made-china-how-instant-loan-app-racket-boomed-india-141331> accessed 4 February 2021.
11 "Regulation of Mobile Lending Entities in Kenya | MMAN ADVOCATES" (Mman.co.ke, 2019) <https://mman.co.ke/content/regulation-mobile-lending-entities-kenya> accessed August 31, 2020 Mwakaneno Gakweli, "Kenya's Central Bank Drafts New Laws to Regulate Non-Bank Digital Loans" (Kenyan Wallstreet , July 20, 2020) <https://kenyanwallstreet.com/cbk-to-regulate-mobile-loans-in-new-law/> accessed August 31, 2020.
12 This was contained in a petition filed by a member of the Kenyan Parliament to the Central Bank of Kenya, asking the apex bank to regulate digital lending platforms. Available here "Unemployed Kenyans to Be Blocked From Loan Apps" (Kenyans.co.ke , 2020) <https://www.kenyans.co.ke news/50819-unemployed-kenyans-be-blocked-loan-apps> accessed August 31, 2020.
13 'Made in China: How the Instant Loan App Racket Boomed in India' (The News Minute , 12 January 2021) <https://www.thenewsminute.com/article/made-china-how-instant-loan-app-racket-boomed-india-141331> accessed 4 February 2021.
14 CBN Unveils Draft Guidelines For Micro Finance Banks.https://thewillnigeria.com/news/cbn-unveils-draft-guidelines-for-micro-finance-banks/
15 Section 124 of FCCPA
16 Section 127 of FCCPA
17 Section 114 of FCCPA
18 It is an offence under Section Section 24 (2) (c) of the Cybercrimes Act 2015 to issue threats to harm the reputation of another individual.
19 Section 34 of the Constitution of the Federal Republic of Nigeria 1999.
20 Economic and Financial Crimes Commission. The Nigerian government agency responsible for investigating and prosecuting financial crimes.
21 In the case, the court chastised the Police for being a willing tool for harassment. Ogbonna v Ogbonna (2014) LPELR-22308(CA)
22 Consent is the appropriate lawful basis for this type of processing.
23 Section 5.5.7 of the CBN Consumer Protection Regulation.
24 Section 5.5.7. (b) of the CBN Consumer Protection Regulation.
25 Section 7 of CBN Consumer Protection Guideline on Responsible Business Conduct.
26 Section 114 of FCCPA
27CBN Anti-Money Laundering and Counter Terrorism Finance Manual - https://www.cbn.gov.ng/OUT/CIRCULARS/BSD/2009/CIRCULAR%20ON%20CBN%20AMLCFT%20MANUAL.PDF See also Central Bank of Nigeria (Anti-money Laundering and Combating Financing of Terorism in Banks and Other Financial Institutions in Nigeria) Regulations -https://www.cbn.gov.ng/out/2014/fprd/aml%20act%202013.pdf and Money Laundering (Prohibition) Act -https://lawpadi.com/wp-content/uploads/2015/08/Money-Laundering-Act-2011.pdf
28 Section 127 of FCCPA and Section 3.3 of CBN's Consumer Protection Regulation
29 Section 127 (2) (a) & (b) of FCCPA
30 Section 114 of FCCPA
31 Section 124 of FCCPA
32 'Opera: Phantom of the Turnaround – 70% Downside' (Hindenburg Research , 16 January 2020) <https://hindenburgresearch.com/operaphantom-of-the-turnaround/> accessed 4 February 2021.
33 'Financial Products and Services - Advertising Policies Help' <https://support.google.com/adspolicy/answer/2464998?hl=en> accessed 4 Febr uary 2021.
34 Section 125 of FCCPA
35 According to Google Play Developer Distribution Agreement: "you will protect the privacy and legal rights of users. If the users provide You with, or Your Product accesses or uses, usernames, passwords, or other login information or personal information, You agree to make the users aware that the information will be available to Your Product, and You agree to provide legally adequate privacy notice and protection for those users. Further, Your Product may only use that information for the limited purposes for which the user has given You permission to do so. If Your Product stores personal or sensitive information provided by users, You agree to do so securely and only for as long as it is needed. "Google Play" (Google.com , 2020) <https://play.google.com/about/developer-distribution-agreement.html> accessed January 19, 2021
36 Consent of a User is required before direct marketing. Article 5.3.1 (a) of the DPIF. 'Data Hawking and the Economics of Perversion' (CybersecFill 7 November 2020) <https://www.cybersecfill.com/data-hawking-and-economics-of-perversion/> accessed 30 January 2021.
37 Some of the third parties that own the trackers disclosed in their privacy notice they also share the data with other third parties.
38 'This Lending App Loves You until You're Late on a Payment. Then the Shaming Begins.' (Rest of World , 26 May 2020) <https://restofworld.org/2020/okash-microlending-public-shaming/> accessed 4 January 2021. 39 The Norwegian Data Protection Authority (Datatlsynet) issued a notice of intention to fine Grindr the sum of 10 million Euros for unlawfully sharing the data with third parties for marketing purposes. According to Datatlsynet, " users were forced to accept the privacy policy in its entirety to use the app, and they were not asked specifically if they wanted to consent to the sharing of their data with third parties. 'Intention to Issue € 10 Million Fine to Grindr LLC' (Datatilsynet) <https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/> accessed 28 January 2021.

40 NITDA has issued Adequacy decisions to a number of countries and it is contained in Appendix 3 of the DPIF.
41 In India, before a government imposed ban, a number of the LendTechs were from China or used as a front for Chinese investors. 'Made in China: How the Instant Loan App Racket Boomed in India' (The News Minute , 12 January 2021) <https://www.thenewsminute.com/article/made-china-how-instant-loan-app-racket-boomed-india-141331> accessed 4 February 2021. Yomi Kazeem, 'A Chinese Super App Is Facing Claims of Predatory Consumer Lending in Nigeria, Kenya and India' (Quartz Africa) <https://qz.com/africa/1788351/operas-okash-opesas-predatory-lending-in-nigeria-india-kenya/> accessed 4 February 2021.
42 Moving data to countries with poor human rights records without sufficient safeguard is risky. In addition, NITDA did not publish its rationale for granting some of these countries an adequacy decision when it is clear they have poor human rights record.
43 Art. 3.1 (2) of the NDPR
44 Article 3.1 (7) of the NDPR
45 Article 2.5 of the NDPR and Article 3.2 (iii) of DPIF
46 "Google Developer Program Policy; User Data - Play Console Help" (Google.com , 2018) <https://support.google.com/googleplay/android-developer/answer/10144311?visit_id=637466601490168212-3911275455&rd=1> accessed January 19, 2021
47 Art. 2.5 of the NDPR
48 Article 5.6 of DPIF requires information about cookies should be provided.
49 The purpose of many of the most common trackers is behaviourally targeted advertising, whereby individuals are evaluated along demographic and behavioural dimensions to determine their propensity to respond to certain marketing messages. Binns R and others, "Third Party Tracking in the Mobile Ecosystem" [2018] Proceedings of the 10th ACM Conference on Web Science - WebSci '18 <https://arxiv.org/pdf/1804.03603.pdf>
50 A User activity can be linked and identified uniquely across both web and mobile apps.
51 Binns R and others, "Third Party Tracking in the Mobile Ecosystem" [2018] Proceedings of the 10th ACM Conference on Web Science - WebSci '18 <https://arxiv.org/pdf/1804.03603.pdf>
52 'New study: The advertising industry is systematically breaking the law' (Forbrukerrådet , 14 January 2020) <https://www.forbrukerradet.no/side/new-study-the-advertising-industry-is-systematically-breaking-the-law/> accessed 28 January 2021.
53 ibid.
54 Some plugins like Privacy badger or Adblockers work effectively well to block tracking on web browsers
55 Browsers like Mozilla and Brave offer users a setting that puts them in control of what to accept or otherwise.
56 "Permissions on Android | Android Developers" (Android Developers , 2020) <https://developer.android.com/guide/topics/permissions/overview> accessed January 17, 2021
57 Though the National Information Technology Development Agency (NITDA) in its capacity as the Data Protection Authority is yet to issue any Guidance on profiling, insight can be drawn from the Article 29 Working Party (Now European Data Protection Board) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. "ARTICLE29 Newsroom - Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01) - European Commission" (Europa.eu , November 4, 2016) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed January 19, 2021
58 Norwegian Consumer Council, 'OUT OF CONTROL: How Consumers Are Exploited by the Online Advertising Industry' (2020) <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf> accessed 28 January 2021.
59 "Permissions on Android | Android Developers" (Android Developers, 2020) <https://developer.android.com/guide/topics/permissions/overview> accessed January 17, 2021
60 "Permissions on Android | Android Developers" (Android Developers , 2020) <https://developer.android.com/guide/topics/permissions/overview> accessed January 17, 2021
61 Android Permissions That Need a Privacy Policy - TermsFeed. https://www.termsfeed.com/blog/android-permissions-privacy-policy/
62 Developer Program Policy (effective December 16, 2020 .https://support.google.com/googleplay/android-developer/answer/10286120?hl=en
63 Navigating away from the disclosure does not constitute consent, likewise, auto-dismissing or expiring messages are not valid consent.
64 App developers are mandated to "respect users' decisions if they decline a request for a Restricted Permission, and users may not be manipulated or forced into consenting to any non-critical permission. You must make a reasonable effort to accommodate users who do not grant access to sensitive permissions (e.g., allowing a user to manually enter a phone number if they've restricted access to Call Logs)."
65 Article 2.6 of the NDPR
66 High-Tech Bridge, HTBridge/Pivaa (2021) <https://github.com/HTBridge/pivaa> accessed 28 January 2021.
67 ibid.
68 'Going Old Fashion: Debugging Android with JDWP (Day 6) , Smali Is Drinking Rootbeer(Android memory forensic analysis with LIME volatility (Day 5) (work on progress)) <https://court-of-testing-analysing.blogspot.com/2018/11/android-memory-forensic-analysis-with.html> accessed 28 January 2021.
69 "Financial Services - Play Console Help" (Google.com , 2018) <https://support.google.com/googleplay/android-developer/answer/9876821?hl=en> accessed January 20, 2021
70 Section 127 of FCCPA and Section 3.3 of the CBN Consumer Protection Regulation
71 'How Predatory Loan Apps Preyed on Cash-Strapped Indians And Abused Their Data' <https://www.vice.com/en/article/4ad5bw/how-loan-apps-weaponise-your-data-to-make-you-pay> accessed 4 February 2021. 72 Section 114 of the FCCPA and Section 4.1 of the C CBN Consumer Protection Regulation mandates that information should be provided in plain and understandable language, and displayed in a conspicuous manner.
73 "Dark Patterns" (Darkpatterns.org , 2020) <https://darkpatterns.org/> accessed November 19, 2020
74 Brownlee J, "Why Dark Patterns Won't Go Away" (Fast Company , August 22, 2016) <https://www.fastcompany.com/3060553/why-dark-patterns-wont-go-away> accessed November 19, 2020
75 "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites" (Princeton.edu , 2019) <https://webtransparency.cs.princeton.edu/dark-patterns/> accessed November 19, 2020
76 There is evidence for dark patterns as a third-party service. Ibid.
77 'Dark Design: The Art of Deception by Design' (TechHive Advisory, 26 November 2020) <https://techhiveadvisory.org.ng/dark-design-the-art-of-deception-by-design/> accessed 30 January 2021.
78 Lomas N, "WTF Is Dark Pattern Design?" (TechCrunch , July 2018) <https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/> accessed November 3, 2020
79 "Using the Manipulation Matrix for Ethical Behavioral Design | Designli Blog" (Designli Blog , November 15, 2018) <https://designli.co/blog/using-the-manipulation-matrix-for-ethical-behavioral-design/> accessed November 6, 2020

80 "The New Physics of Financial Services" http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf accessed January 17, 2021
81 Klein A, "Reducing Bias in AI-Based Financial Services" (Brookings , July 10, 2020) <https://www.brookings.edu/research/reducing-bias-in-based-financial-services/> accessed January 17, 2021.
82 "Black Loans Matter: Fighting Bias for AI Fairness in Lending - MIT-IBM Watson AI Lab" (MIT-IBM Watson AI Lab , December 14, 2020) <https://mitibmwatsonailab.mit.edu/research/blog/black-loans-matter-fighting-bias-for-ai-fairness-in-lending/> accessed January 17, 2021.
83 This is based on information made publicly available in media release, their respective website and other media channels profiling the product.
84 Art. 3.1 (7) (L) of the NDPR mandates that the information about automated processing and logic should be provided in the privacy notice. See also Art. 3.2 (xvi) of DPIF. Art. 5.3.1 (f) of DPIF requires that consent of the data subject should be gotten before making a decision based solely on automated Processing which produces legal effects concerning or significantly affecting the Data Subject.
85 Bartneck C and others, "Privacy Issues of AI" [2020] An Introduction to Ethics in Robotics and AI 61 <https://link.springer.com/chapter/10.1007/978-3-030-51110-4_8> accessed January 17, 2021.
86 Article 2.12 of the NDPR
87 Article 4.2 (b) of DPIF
88 Article 4.2 (d) of DPIF
89 Article 4.1 (2) of the NDPR
90 "Deceptive Behavior - Play Console Help" (Google.com , 2018) <https://support.google.com/googleplay/android-developer/answer/9888077?hl=en&ref_topic=9877467#zippy=%2Cexamples-of-common-violations> accessed January 19, 2021
91 "Unemployed Kenyans to Be Blocked From Loan Apps" (Kenyans.co.ke , 2020) <https://www.kenyans.co.ke/news/50819-unemployed-kenyans-be-blocked-loan-apps> accessed August 31, 2020
92 Section 5.2 of the CBN Consumer Protection Regulation.
93 Section 105 (2) of the FCCPA
94 This is similar to the regulatory oversight played by the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act, which empowers the FTC to sanction organisations for privacy violation.
95 A lot can be learnt from the provision of the Fair Debt Collection Practices Act (FDCPA) of the United States.
96 The Bill has scaled the second reading at the Senate and awaiting the Senate Committee Report.
97 Interestingly, Nigeria has had a Credit Reporting Act since 2017.
98 "Google Removes Personal Loan Apps From Play Store For Violating User Safety Policies" (https://www.outlookindia.com/ , January 14, 2021) <https://www.outlookindia.com/website/story/business-news-google-removes-personal-loan-apps-violating-user-safety-policies-from-play-store/370520> accessed January 19, 2021
99 Google removed 600 Apps on PlayStore for inappropriate placement of Ads. Catalin Cimpanu, "Google Removes 600 Android Apps in Play Store Adware Crackdown" (ZDNet , February 20, 2020) <https://www.zdnet.com/article/google-removes-600-android-apps-in-play-store-adware-crackdown/> accessed January 19, 2021
100 Apple is stepping up privacy requirements on its App Store, which will force developers to be more transparent about data processing with consequences of being removed for default. The initiative is described as App Tracking Transparency, it will require apps to clearly ask for users' permission before tracking them. Chan K, "Apple to Tighten App Privacy, Remove Apps That Don't Comply" (AP NEWS , December 8, 2020) <https://apnews.com/article/apple-inc-software-890abfaaf67fd39f2c1ca65f9bc1a924> accessed January 19, 2021 101 Dangerous permissions and hidden trackers in your period .https://techcabal.com/2020/10/08/hidden-trackers-permissions-period-apps-nigeria/
102 Why does V&H Android app has so many trackers injected .https://villagersandheroes.com/forums/threads/why-does-v-h-android-app-has-so-many-trackers-injected-into-it.2975/
103 Our Android App's Permissions Explained – ottonova Tech. https://ottonova.tech/our-android-apps-permissions-explained/
104 [Tutorial] [Android] [IOS] HOW TO ASK FOR USER PERMISSION .https://medium.com/codespace69/tutorial-android-ios-how-to-ask-for-user-permission-in-flutter-part-1-91681027d635
105 "Application Security | Android Open Source Project" (Android Open Source Project, 2020) <https://source.android.com/security/overview/app-security> accessed January 17, 2021
106 "Understanding Permissions in the Android World | CleverTap" (CleverTap, 2018) <https://clevertap.com/blog/understanding-android-permissions/> accessed January 17, 2021
107 "Referrer Policy" (W3.org , January 26, 2017) <https://www.w3.org/TR/referrer-policy/> accessed Nov 2, 2020
108 The Ultimate Guide Of Mixed Content SSL Warnings In. https://wpuber.com/the-ultimate-guide-of-mixed-content-ssl-warnings-in-wordpress-2020/
109 "What Is SSL (Secure Sockets Layer)? | DigiCert.Com" (DigiCert , 2017) <https://www.digicert.com/ssl/#:~:text=Secure%20Sockets%20Layer%20(SSL)%20is,client%20(e.g.%2C%20Outlook).> accessed August 31, 2020
110 The Ultimate Guide Of Mixed Content SSL Warnings In .https://wpuber.com/the-ultimate-guide-of-mixed-content-ssl-warnings-in-wordpress-2020/
111 The Ultimate Guide Of Mixed Content SSL Warnings In .https://wpuber.com/the-ultimate-guide-of-mixed-content-ssl-warnings-in-wordpress-2020/
112 "Content Security Policy (CSP)" (MDN Web Docs , Nov 2, 2020) <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP> accessed May 12, 2020
113 Content Security Policy (CSP) - HTTP | MDN. https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
114 Ibid.

Ikigai
Innovation
Initiative

TECH HIVE
ADVISORY

regcompass

Naijasecforce

Digital Lending: Inside the Pervasive Practice of LendTechs in Nigeria