NIGERIAN COMMUNICATIONS COMMISSION

FEDERAL UNIVERSITY OF TECHNOLOGY MINNA
Technology for Empowerment

NIGERIAN DIGITAL CONSUMER PROTECTION

HANDBOOK

A Production of NCC Professorial Chair Endowment
at Federal University of Technology, Minna.

Nigerian Digital Consumer Protection

HANDBOOK

From The Professor's Desk

The Nigerian Communications Commission (NCC) has established an endowment to promote research and development in the communications industry, with a focus on Engineering, Computer Science, Information and Communications Technology (ICT), and the Social Sciences. The Federal University of Technology, Minna (FUTMinna) has been recognized as the lead institution in this initiative.

The endowment is strategically directed towards four key areas:

1. Developing Nigeria's capacity for 6G and Light-Fidelity (Li-Fi).
2. Assessing the impact of Big Data Analytics and Artificial Intelligence on Nigeria's digital economy.
3. Enhancing consumer protection in the digital era.
4. Supporting ICT projects in unserved and underserved regions.

This Handbook on Nigerian Digital Consumer Protection is one of the initiatives under the Chair focused on enhancing consumer protection in the digital era. It is a product of research and findings, designed to advance the efforts of the Nigerian Communications Commission.

Looking ahead, the team plans to integrate Artificial Intelligence and updated case scenarios into subsequent editions of the handbook. Additionally, efforts will be made to create an online version within our Learning Management System, ensuring well-meaning Nigerians—especially MSMEs and vulnerable groups—have access to this wholesome and educative resource.

Indeed, there is always something new to learn.

Professor Abraham U. Usman
Team Lead, NCC Professorial Chair Endowment, FUT Minna

FOREWORD

In today's interconnected world, the digital space is no longer optional; it is the backbone of how we learn, work, trade, and socialize. For millions of Nigerians, particularly our youth, every financial transaction, academic pursuit, and social interaction now leaves a digital footprint. While this transformation offers immense opportunity, it also presents profound risks. Online fraud, identity theft, data breaches, predatory loan apps, and algorithmic bias are no longer distant problems; they are daily realities for Nigerian consumers.

The Nigerian government, through regulatory institutions such as the Nigerian Communications Commission (NCC), the National Information Technology Development Agency (NITDA), and the recently established Nigeria Data Protection Commission (NDPC), has taken steps to build a robust framework for digital consumer rights. The passage of the **Nigeria Data Protection Act (NDPA) 2023** marked a significant milestone in recognizing that personal data is not just information, but a form of identity and dignity that must be safeguarded. Nevertheless, laws and policies alone cannot protect consumers. Awareness, digital literacy, and self-defense skills remain the first and strongest line of defense.

This handbook is therefore both timely and essential. It speaks directly to Nigerian students, youth, and everyday consumers, equipping them with the tools they need to navigate the digital economy safely and securely. From understanding what personal data is to learning how to activate two-factor authentication (2FA), manage app permissions, or report fraud, the handbook transforms complex regulatory language into practical guidance for daily life. It also engages critical debates around **artificial intelligence, fairness, and governance**, ensuring that young Nigerians are not just passive users of technology but informed participants in shaping its future.

As we continue to build a resilient digital economy, consumer protection must remain a central focus. A secure, transparent, and fair digital

environment will not only protect citizens but also inspire confidence, attract innovation, and strengthen Nigeria's global competitiveness.

I commend the authors of this handbook for their clarity, practicality, and vision. I hope that every reader, student, entrepreneur, professional, or policymaker will find in these pages both guidance and empowerment. For in the digital age, ***to be informed is to be protected, and to be protected is to be empowered***.

Prof. Abiodun Musa Aibinu,
Vice-Chancellor/Chief Executive and Academic Officer,
Summit University, Offa,
Kwara State, Nigeria.

Table of Contents

From The Professor's Desk.....ii

FOREWORD iii

CHAPTER 1..... 2
Introduction: Why Digital Protection Matters..... 2
1.1 The Digital Footprint of Everyday Life..... 2
1.2 Opportunities and Risks in Nigeria's Digital Space..... 2
1.3 Building Digital Resilience 3
1.4 Summary: Towards Digital Empowerment 3

CHAPTER 2..... 5
Understanding the Data Economy: Data Economy the New Oil for Nigeria 6
1.5 What is Personal Data? 6
1.6 Types of Personal Data..... 7
1.7 How Nigerian Platforms Collect Your Data 9
1.8 Data Monetization Explained Simply..... 11
1.9 Summary: Personal Data – Nigeria's New Digital Asset 13

CHAPTER 3..... 14
AI & Consumer Risks..... 15
1.10 🔍 What is AI Profiling?..... 15
1.11 How Algorithms Assign Scores and Labels..... 15
1.12 The Danger of Bias in AI Systems 18
1.13 Predictive Policing, Auto-Denials & Unfair Pricing Models 19
1.14 Summary: AI & Consumer Protection Risks in Nigeria..... 21

CHAPTER 4 23
Data Protection Laws & Rights 23
4.1 The Nigerian Data Protection Act (NDPA) 2023 24
4.2 Your Digital Rights as a Nigerian Consumer 24
4.3 Key Regulators Protecting You 25
4.4 Challenges with Enforcement in Nigeria 27
4.5 Summary for Consumers 28
4.6 Summary: Protecting Personal Data & Consumer Rights in Nigeria 29

CHAPTER 5 30
Tools for Digital Self-Defense 31
5.1 Why Personal Digital Safety Matters 31
5.2 Core Digital Safety Tools: Step-by-Step Guides 31
5.3 🌍 Safe Use of Public Wi-Fi & Social Media 36
5.4 Summary: Building Everyday Digital Resilience 40

CHAPTER 6 41
Digital Rights for Students & Youth 42
5.5 Understanding Digital Rights 42
5.6 Building Campus Awareness 43
5.7 Advocacy and Peer Education 44
5.8 Summary: Empowering the Digital Generation 46

CHAPTER 7 47
Future of AI & Governance in Nigeria 48
5.9 Understanding AI and Its Impact 48
5.10 Explainable AI: Why Transparency Matters 48
5.11 Balancing Regulation and Innovation 49
5.12 Multi-Stakeholder Governance 50
5.13 Summary: Shaping an Inclusive AI Future 51

CHAPTER 8 52
Call to Action 53
5.14 Taking Personal Responsibility 53
5.15 The 10 Commandments of Digital Consumer Protection .. 53
5.16 Resources & Hotlines for Complaints / Reporting Fraud in Nigeria 54
5.17 Summary: Becoming a Digital Protector 55

CHAPTER 9 57
Further Reading 57
9.1 Nigerian Regulatory and Policy Documents 57
9.2 International Guidelines 58
9.3 Academic and Research Sources 59
9.4 Case Studies and Reports 59

References 60

CHAPTER 1

Introduction: Why Digital Protection Matters

Authors/Contributors: A. U. Usman; S. Zubair; A. A. Sadiq; A. O. Abdulbaki

Summary: Towards Digital Empowerment

Digital safety is everyone's duty. With awareness, peer education, and support from bodies like NCC and NITDA, Nigerians can enjoy technology responsibly. By following the "10 Commandments of Digital Consumer Protection" and knowing key hotlines, every user can stay informed and secure.

In short: *this is not just a manual for avoiding fraud. It is a roadmap for digital empowerment—so that Nigerian students, youth, and consumers can take control of their online lives, safeguard their futures, and shape the digital economy on their own terms.*

Digital protection is no longer optional in Nigeria's rapidly evolving digital landscape—it's an essential life skill for every citizen. This handbook serves as both a practical guide for avoiding online threats and a roadmap for digital empowerment, enabling Nigerian students, youth, and consumers to take control of their online lives and shape the digital economy on their own terms.

CHAPTER 1

Introduction: Why Digital Protection Matters

The digital world is now an inseparable part of our daily lives. From banking and education to shopping and entertainment, Nigerians are increasingly dependent on technology for convenience and opportunity. Nevertheless, this rapid digital transformation comes with challenges—ranging from online scams to misuse of personal data.

This handbook begins with an introduction that explains why digital protection matters for every citizen. It outlines the realities of living in a connected society, highlights both the opportunities and risks that come with digital participation, and emphasizes the importance of building resilience. The goal is straightforward: to empower students, young people, and consumers with the knowledge and tools they need to thrive safely in Nigeria's digital economy.

1.1 The Digital Footprint of Everyday Life

We live in a world where almost everything we do leaves a **digital trace**. Each time we use our phones, shop online, transfer money, or post on social media, we share pieces of personal information. For Nigerian consumers, this is particularly important due to the rapid growth of fintech, e-commerce, social media, and mobile banking platforms**.**

1.2 Opportunities and Risks in Nigeria's Digital Space

However, with opportunity comes risk. Fraudsters, careless companies, and even biased AI systems can misuse our data in ways that affect our finances, privacy, and even our dignity. The Central Bank of Nigeria has repeatedly warned about online fraud. Telecom scams, fake investment schemes, and identity theft are now everyday threats. At the same time, government policies and corporate practices sometimes ignore consumer rights, leaving young people especially vulnerable.

1.3 Building Digital Resilience

Protecting yourself online is no longer optional—it is part of being **a** responsible digital citizen. Whether it is learning how to set up two-factor authentication, joining a digital literacy club on campus, or knowing where to report fraud, digital self-defense is an essential life skill**.**

The digital space shapes how we learn, work, and connect, but it also presents risks such as scams and data misuse. Staying safe online means knowing the right tools, understanding our rights, and holding institutions accountable.

This digital consumer protection handbook is designed as a guide to:

- Provide step-by-step tools for online safety (from using password managers to avoiding scams on public Wi-Fi).
- Explain why digital rights matter for students, youth, and the generality of 'digital consumers' in Nigeria, and how peer education can drive change.
- Explore the future of AI and governance, highlighting the role of NCC, NITDA, and civil society in protecting consumers while fostering innovation.
- End with a clear call to action: thereby outlining "***10 Commandments of Digital Consumer Protection***" and a list of hotlines every Nigerian should know.

1.4 Summary: Towards Digital Empowerment

Digital safety is everyone's duty. With awareness, peer education, and support from bodies like NCC and NITDA, Nigerians can enjoy technology responsibly. By following the "10 Commandments of Digital Consumer Protection" and knowing key hotlines, every user can stay informed and secure.

In short, this is not just a manual for avoiding fraud. It is a roadmap for digital empowerment—enabling Nigerian students, youth, and consumers to take control

of their online lives, safeguard their futures, and shape the digital economy on their own terms.

Digital protection is no longer optional in Nigeria's rapidly evolving digital landscape—it is an essential life skill for every citizen. This handbook serves as both a practical guide for avoiding online threats and a roadmap for digital empowerment, enabling Nigerian students, youth, and consumers to take control of their online lives and shape the digital economy on their own terms.

CHAPTER 2

Understanding the Data Economy: Data Economy, the New Oil for Nigeria

Authors/Contributors: *C. A. Alenoghena; T. A. Folorunso; S. Zubair; C. Innocent*

Summary: Personal Data – Nigeria's New Digital Asset

Your personal data is valuable currency in today's digital economy. Nigerian companies collect and monetize this data daily through advertising, profiling, and targeted sales. Case studies from Nigeria demonstrate how data misuse can lead to fraud, harassment, and security risks. The challenge remains that while companies profit from your data, consumers are often left unprotected—making digital consumer protection an urgent priority.

CHAPTER 2

Understanding the Data Economy: Data Economy the New Oil for Nigeria

Around the world, conversations about wealth and power are no longer limited to natural resources. Data now stands alongside oil and gold as a critical asset that drives economies and shapes societies. In Nigeria, where digital services—from banking to social media—are integral to everyday life, understanding the data economy is crucial for protecting citizens and promoting fair growth.

The digital world is built on data. Every message you send, every payment you make, and every time you browse the internet, you leave behind information. This information, called data, has become as valuable as oil or gold. Businesses, governments, and even criminals want it because it can be used to generate revenue, inform decisions, or influence behavior.

1.5 What is Personal Data?

Personal data is any information that can be used to identify you directly or indirectly. It is also known as personal information or personally identifiable information (PII), which is any information that relates to an identified or identifiable living person. This means information that can be used on its own, or in combination with other information, to pinpoint a specific individual.

This concept is central to data protection laws worldwide, including in Nigeria, with the *Nigeria Data Protection Act (NDPA) 2023*. These laws are designed to protect a person's privacy and give them control over how their data is collected, used, and stored.

- **How is a person "identifiable"?** An individual can be identified directly or indirectly.
    - **Directly:** This is when the information itself clearly points to a person.

Examples: Full name, home address, National Identity Numbers (NIN), Bank Verification Number (BVN), Social Security Number (SSN), or International Passport Number.

- **Indirectly:** This is when a piece of information, when combined with other data, can identify a person.

Examples: An IP address, an employee ID, or a series of online browsing habits can become personal data when they are linked to a specific person.

1.6 Types of Personal Data

Personal data shapes how people are identified, tracked, and understood in the digital space. Some information is fairly routine, while other details are deeply private and carry serious risks if mishandled. Recognizing the difference is key to understanding why certain data demands stronger protection under Nigerian law.

Personal data can be categorized into two main types

1. **General Personal Data:** This broad category encompasses a wide range of information.
   - ***Examples:***
   - **Contact Information:** Name, email address, phone number.
   - **Identifiers:** Identification numbers (BVN, NIN, etc.), online identifiers (IP address, cookie ID).
   - **Demographic Data:** Age, gender, nationality, marital status.
   - **Financial Information:** Bank account number, credit card details, and salary information.
   - **Employment Details:** Job title, employer, work address.
   - **Online Activity:** Browsing history, app usage statistics, search queries.
2. **Sensitive Personal Data (or Special Categories of Data):** This is information that, if exposed, could lead to significant harm or

discrimination. Data protection laws, like Nigeria's NDPA, provide a higher level of protection for this type of data.

- ***Examples:***

- Racial or ethnic origin.
- Political opinions or affiliations.
- Religious or philosophical beliefs.
- Trade union membership.
- **Genetic Data:** Data from DNA analysis.
- **Biometric Data:** Fingerprints, facial recognition data, and voice patterns used for identification.
- **Health Data:** Medical records, information about physical or mental health conditions.
- Data concerning an individual's sex life or sexual orientation.

Everyday details, such as contact information, financial records, or online activity, fall under general personal data, as shown in Table 1. Although these are widely collected, they still require protection from misuse. Sensitive data, however, covers information like health, biometrics, or political beliefs, where exposure could lead to discrimination or harm. This is why laws like the NDPA give it higher safeguards. At its core, personal data protection is about safeguarding individuals and ensuring their dignity and privacy remain intact in a digital world.

Table 1: Types of Personal Data

General Personal Data (Examples)	Sensitive Personal Data (Examples)
Name, Email, Phone Number	Health Records
Age, Gender, Nationality	Biometrics (fingerprints, facial data)
BVN, NIN, IP Address	Political or Religious Beliefs
Employment Details	Genetic Data

It is important to note that information about companies, businesses, or legal entities is not considered personal data. Personal data applies only to information about a living, natural person.

Case Study–SIM Registration Leak: In 2020, reports emerged that SIM registration details of Nigerians were being sold illegally for as low as ₦100 on the street. These details included names, addresses, and photos collected during SIM registration. Criminals used this stolen personal data to carry out fraud and impersonation.

1.7 How Nigerian Platforms Collect Your Data

Across Nigeria's digital economy, data collection has become a routine practice. Whether it is signing up for an app, ordering food, or logging into social media, platforms gather personal details — sometimes openly with consent, and other times quietly in the background.

Most Nigerian digital platforms and service providers collect personal data — often with your consent (like when you sign up for an app), and sometimes quietly in the background.

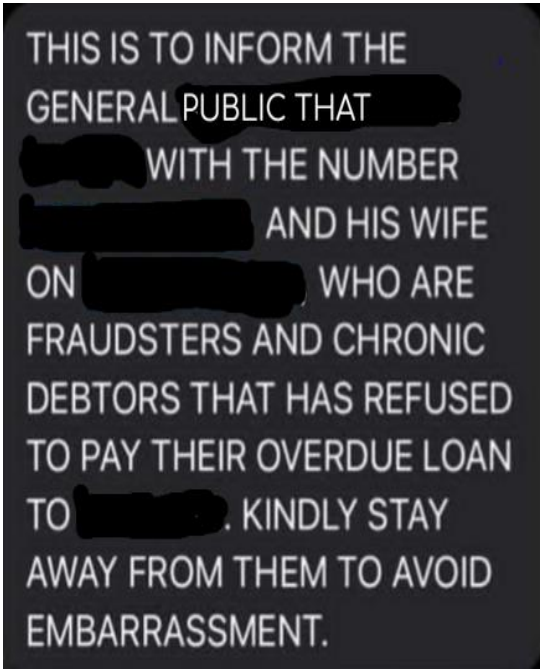
- **Telecom Companies (MTN, Airtel, Glo, 9mobile):** Collect your name, SIM registration details, call history, SMS logs, and internet usage.
- **Fintech & Banks (Opay, Kuda, GTBank, Access Bank):** Collect your BVN, NIN, transaction history, spending patterns, and even your device location.
- **E-commerce (Jumia, Konga):** Track what items you search for, what you buy, how much you spend, and your delivery addresses.
- **Ride-hailing & Food Delivery (Bolt, InDrive, Glovo):** Collect GPS location data, payment details, and travel patterns.
- **Social Media (Facebook, Instagram, TikTok, Twitter/X):** Collect your posts, likes, comments, followers, and even analyze your facial data from photos.

Telecom operators, banks, fintech companies, e-commerce sites, ride-hailing apps, and social media platforms all collect consumer information, including call history, spending patterns, GPS locations, and even facial data. While this fuels services and innovation, it also

raises serious concerns about privacy, security, and the extent to which individuals truly have control over their own information.

Case Study – Loan Apps & Contact List Abuse:

In the year 2021–2022, many Nigerians complained that unlicensed loan apps were accessing their phone contact lists. When borrowers delayed repayment, these apps sent shaming messages to friends, family, and colleagues, as shown in Figure 1. This abuse of personal data led to public outcry, and the Federal Competition and Consumer Protection Commission (FCCPC) eventually took action against several apps.



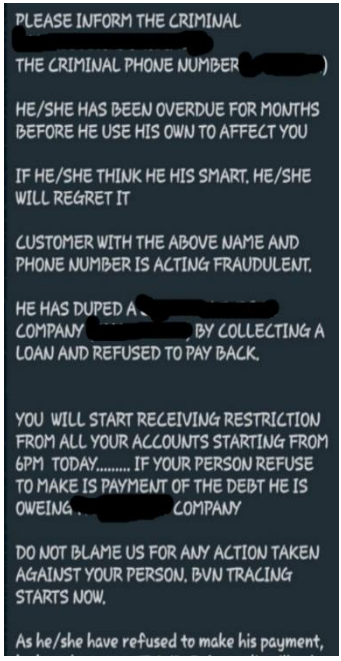


Figure 1: Examples of unlicensed loan companies shaming their customers

1.8 Data Monetization Explained Simply

So why do companies want your data? The answer is simple: data = money**.**

The data collected by Nigerian companies is rarely stored idly — it is actively turned into profit. Businesses rely on this information to shape how they advertise, categorize, and sell to consumers, often in ways that people do not fully realize.

Companies use your data in three main ways:

1. **Advertising (Ads):**
    - Ever searched for shoes on Jumia and suddenly started seeing shoe ads on Facebook?
    - That is because companies sell or share your browsing history with advertisers.

    ⚠ **Case Study – Targeted Ads Scandal:**
    In 2019, Nigerian Facebook users noticed political ads targeting specific tribes and regions during the elections. This was possible because advertisers bought access to people's online behaviors and locations.

2. **Profiling:**
    - Platforms group people into categories: "students," "low spenders," "frequent travelers."
    - These profiles are then used to target you with specific offers — or to deny you certain services.

    💡 **Example:** A fintech may tag you as "risky" if your income is irregular, reducing your chances of getting a loan — even if you have never defaulted.

3. **Targeted Sales:**
    - If Opay notices you buy airtime every Friday night, it might push a Friday airtime discount to you.

- If GTBank sees regular transfers to a betting app, it may flag your account as "high risk" for credit services.

Through advertising, profiling, and targeted sales, companies transform personal data into a powerful marketing tool. While this creates convenience and tailored offers, it can also fuel manipulation, unfair treatment, and exclusion. Nigerian case studies — from political ad targeting to loan denials — demonstrate how these practices directly impact consumers, underscoring the importance of transparency and regulation.

> ⚠ **Case Study – MTN Nigeria Fine (2015):**
>
> The NCC fined MTN $5.2 billion for failing to disconnect unregistered SIM cards. One reason was that unverified data posed national security risks and could be misused for fraud or terrorism. This highlighted the critical importance of consumer data in Nigeria's economy.

Personal data has become the new oil of the digital economy. Every click, call, or purchase leaves a trace — and Nigerian companies harvest this information daily. While data drives services and profits, its misuse can expose consumers to fraud, harassment, and even national security risks.

- Your personal data is valuable — almost like currency.
- Nigerian companies collect it daily when you use their services.
- They monetize it by selling ads, profiling customers, and targeting sales.
- Case studies in Nigeria show how data misuse can lead to fraud, harassment, and even national security risks.

Your data is currency, and in Nigeria, it is constantly collected and monetized. From targeted ads to risky profiling, the stakes are high when protection is weak. Real-life cases show why consumers must stay alert and why stronger safeguards are urgently needed.

☞**The challenge is:** while companies' profit, consumers are often left unprotected, which is why digital consumer protection is urgent.

1.9 Summary: Personal Data – Nigeria's New Digital Asset

Your personal data is valuable currency in today's digital economy. Nigerian companies collect and monetize this data daily through advertising, profiling, and targeted sales. Case studies from Nigeria demonstrate how data misuse can lead to fraud, harassment, and security risks. The challenge remains that while companies profit from your data, consumers are often left unprotected—making digital consumer protection an urgent priority.

CHAPTER 2

AI & Consumer Risks

Authors/Contributors: *B. A. Salihu, J. A. Bala; T. A. Mamman*

Summary: AI & Consumer Protection Risks in Nigeria

AI decisions increasingly affect who gets loans, service pricing, and even personal identification in Nigeria. Bias in AI systems can lead to unfair treatment, particularly affecting students, low-income earners, and marginalized groups. Real-life Nigerian examples show these risks are not theoretical—they're happening now. Understanding these challenges is essential for demanding transparency and accountability from AI-driven services.

CHAPTER 3

AI & Consumer Risks

Artificial Intelligence is no longer a futuristic concept — it is already woven into daily life in Nigeria. From banking to shopping, transport to social media, AI shapes decisions that affect how people live, work, and spend. Nevertheless, as its influence grows, so do the concerns about fairness, accountability, and consumer protection.

Artificial Intelligence (AI) is becoming part of everyday life in Nigeria, even if you do not notice it. From the apps we use to the way banks approve loans or e-commerce platforms suggest products, AI is quietly making decisions about us. But while AI offers convenience, it also introduces **risks**: unfair treatment, hidden discrimination, and even financial losses. Let us unpack how this works.

1.10 🔍 What is AI Profiling?

Artificial Intelligence (AI) profiling is when computer systems analyze your data—such as phone usage, shopping habits, or social media activity—to make predictions about you. For example, a loan app might analyze how often you recharge airtime or the types of messages you send to decide whether you are "creditworthy."

On the surface, this can make services faster and more convenient. However, when used without transparency, AI profiling can pose significant risks to Nigerian consumers.

1.11 How Algorithms Assign Scores and Labels

Artificial Intelligence often makes decisions by grouping people into categories based on their data, a process known as profiling. This shapes the opportunities and prices consumers face across different digital services in Nigeria.

AI works by analyzing large amounts of data and categorizing people. This process is called **profiling**.

- **Loan Apps:** Decide whether you are a "good" or "bad" borrower by looking at your transaction history, airtime top-ups, or even the contacts on your phone, as illustrated in Figure 2.

Figure 2: Credit score check for loan apps

- **Ride-Hailing Apps:** Decide if you are a "high-demand passenger" and may charge you more during peak hours.
- **E-commerce:** Classify yourself as a "bargain hunter" or "high spender" and adjust the products or discounts you see.

From loan apps labeling borrowers as "good" or "bad," to ride-hailing platforms adjusting fares and e-commerce sites tailoring discounts, AI profiling directly influences everyday digital experiences. While it can create convenience, it also risks unfair treatment when consumers are reduced to data-driven labels without context.

💡 **Case Study – Nigerian Loan Apps:** A student in Lagos applied for a ₦10,000 loan. The app's AI rejected her, not because she had a poor repayment history, but because she did not have a steady salary account. The algorithm automatically labeled her "risky," ignoring her actual creditworthiness and running her crazy, as illustrated in Figure 3.

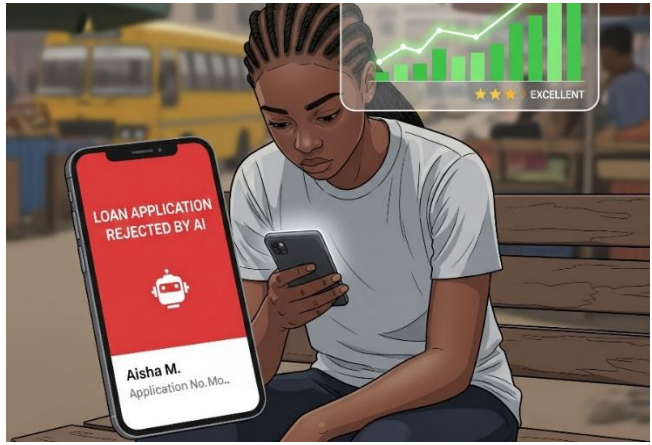


Figure 3: An illustration of the case study

AI is reshaping finance and services in Nigeria, but its decisions are not always fair. When algorithms are biased or opaque, they can lock people out of opportunities without justification.

⚠ Common Risks: Bias, Discrimination, Auto-Denials

While AI promises efficiency and convenience, it also carries serious risks. When flawed or opaque systems drive decisions, consumers can face unfair treatment that directly impacts their opportunities and livelihoods.

1. **Bias in Algorithms**: AI systems "learn" from data, but if the data is flawed or incomplete, the results can be unfair. For example, suppose most past loan applicants came from big cities. In that case, the AI may unfairly score rural applicants as "high risk," even when they have good repayment habits.
2. **Discrimination**: Automated systems can indirectly discriminate based on factors such as gender, age, location, or even the type of phone used. Some Nigerian loan apps have been accused of denying women or students simply because their profiles do not match the "ideal customer" in the AI's dataset.

3. **Auto-Denials Without Explanation**: One of the biggest risks is being rejected for loans, jobs, or services without knowing why. AI systems often give "black box" decisions. Imagine applying for a ₦20,000 digital loan and being denied instantly—yet you have no way to appeal or understand the reason.

Flawed data fuels biased AI, leading to discrimination and unexplained rejections. For Nigerian consumers, this means lost opportunities, unfair treatment, and limited room to challenge decision-making—transparency and accountability in AI systems are urgent.

1.12 The Danger of Bias in AI Systems

Artificial Intelligence is not neutral. If the data it learns from is biased, the decisions will also be biased. AI is only as fair as the data it is trained on. When that data is incomplete or unrepresentative, AI systems inherit and amplify those biases, often with harmful consequences.

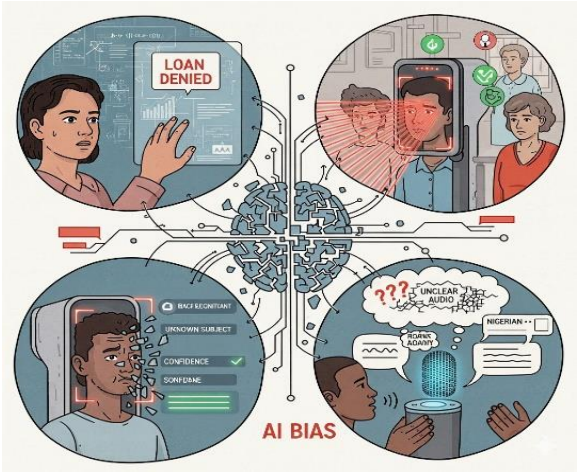


Figure 4: An example of discriminating AI

- **Loan Bias:** People without a salary account may be unfairly excluded.
- **Facial Recognition Errors:** AI struggles with darker skin tones, leading to misidentification as illustrated in Figure 4.

- **Language Bias:** Voice recognition systems may fail to understand Nigerian accents or Pidgin English.

From loan apps excluding people without salary accounts, to facial recognition misidentifying darker skin tones, and voice systems struggling with Nigerian accents, biased AI creates barriers instead of opportunities. Recognizing these flaws is the first step toward demanding fairer, more inclusive technology in Nigeria.

💡 **Case Study – Facial Recognition at Airports:** Several Nigerians have reported that facial recognition at international airports takes longer to verify them compared to lighter-skinned passengers. This shows how global AI systems can discriminate against Africans because they were not trained on diverse datasets.

Thus, studies in the US and UK show that AI facial recognition systems are less accurate for darker skin tones. If similar systems are adopted in Nigeria for security or banking, they could wrongly flag or deny access to people simply because the AI struggles to "recognize" them.

1.13 Predictive Policing, Auto-Denials & Unfair Pricing Models

AI is no longer limited to background processes — it is being applied in areas that directly shape people's lives and opportunities. When used without proper safeguards, these systems can quickly cross into unfair and harmful territory.

AI is increasingly used in sensitive areas that directly affect people's lives:

- **Predictive Policing:** Some countries use AI to predict who might commit crimes. If adopted without caution in Nigeria, such systems could unfairly target youth in certain neighborhoods.
- **Auto-Denials:** Banks or insurance companies may automatically deny services based on AI risk scores, without giving consumers a chance to appeal.

- **Unfair Pricing (Dynamic Pricing):** Ride-hailing apps like Bolt or InDrive change fares based on demand. While this can be efficient, it can also mean two people pay different prices for the same trip simply because one is seen as a "frequent user."

From predictive policing that may target youth to automated service denials and unfair pricing in ride-hailing, AI can easily cross into discriminatory practices. Nigeria must ensure fairness, transparency, and consumer protection as AI adoption continues to grow.

Case Study – Bolt Users in Abuja: During peak hours, some Abuja riders noticed fare surges as high as 300%, while new users got discounted rates for the same trip. The AI was rewarding new customers but punishing loyal ones — an unfair pricing outcome.

Other Nigerian and Global Case Studies

Real-world examples in Nigeria and abroad reveal how AI systems, while useful, can also create serious problems when misapplied. These cases highlight both the benefits and dangers of relying too heavily on algorithms.

- **Loan Apps in Nigeria**

  Many fintech loan apps use AI profiling. Some borrowers have complained that even after repaying on time, their loan limits were reduced because the AI flagged "suspicious" patterns—like frequent airtime borrowing. In some cases, people were auto-rejected with no explanation.

- **Telecom Fraud Detection**

  Telecom companies like MTN and Airtel use AI to detect SIM fraud. While this has reduced scam calls, there have been cases where innocent subscribers had their SIMs wrongly barred, disrupting business and family communication.

- **Global Example: Credit Scoring in China & the US**

In China, AI-based social credit scoring has been criticized for unfairly penalizing people. In the US, AI-driven hiring tools have been found to reject women applicants for tech jobs due to biased data. These examples demonstrate that Nigeria must take action early to prevent similar abuses.

From Nigerian loan apps auto-rejecting borrowers, to telecom fraud systems wrongly blocking SIMs, and global cases of biased credit scoring or hiring tools, the lesson is clear: AI can just as easily exclude and harm as it can protect and assist. Nigeria must learn from these experiences and implement safeguards to prevent such abuses from becoming widespread.

- AI decisions affect who gets loans, how much you pay for services, and even how you are identified.
- Bias in AI systems can lead to unfair treatment of Nigerians — especially students, low-income earners, and marginalized groups.
- Real-life Nigerian examples demonstrate that AI risks are not just a theory; they are happening now.

👉 This is why consumer protection laws, digital literacy, and transparent AI systems are essential in Nigeria's digital economy.

1.14 Summary: AI & Consumer Protection Risks in Nigeria

AI decisions increasingly affect who gets loans, service pricing, and even personal identification in Nigeria. Bias in AI systems can lead to unfair treatment, particularly affecting students, low-income earners, and marginalized groups. Real-life Nigerian examples show these risks are not theoretical—they are happening now. Understanding these challenges is essential for demanding transparency and accountability from AI-driven services.

CHAPTER 4

Data Protection Laws & Rights

Authors/Contributors: *M. David; C. Innocent; T. A. Mamman*

Summary: Protecting Personal Data & Consumer Rights in Nigeria

Your personal data belongs to you, not the companies collecting it. The NDPA 2023 grants you fundamental rights including consent, access, correction, deletion, and redress. Regulatory bodies like NDPC, NCC, NITDA, and CBN exist to protect you, though enforcement is still developing. Awareness of these rights represents your first line of defense—if someone misuses your data, you now have legal backing to act.

CHAPTER 4

Data Protection Laws & Rights

As Nigeria's digital economy expands, the question of who controls personal data has become critical. Around the world, robust data protection frameworks are transforming how companies and governments manage information, with a focus on placing consumers at the center. For Nigeria, this shift is not optional — it is necessary to safeguard trust, encourage innovation, and protect citizens from abuse.

Data protection is now a legal reality in Nigeria, with the NDPA 2023 standing as the country's first full national law on digital rights. By aligning with international standards like the GDPR and the African Union Convention, Nigeria signals that consumers deserve stronger control over how their personal data is collected, stored, and used.

- Nigerian Data Protection Act (NDPA 2023) simplified
- International standards (GDPR, African Union Convention, etc.)
- What rights do Nigerian consumers have?

The NDPA 2023 grants Nigerians rights to consent, access, correction, erasure, and redress, ensuring individuals are no longer powerless in the digital space. With regulators enforcing the law and global standards as reference points, the challenge ahead lies in public awareness and enforcement, so that these rights are not just written on paper but lived in practice.

Many Nigerians are unaware that their personal data is protected by law. Just like your land or car has ownership rights, your data also belongs to you. Companies, banks, and platforms that use your data are **only caretakers** — they must respect rules set by Nigerian laws.

4.1 The Nigerian Data Protection Act (NDPA) 2023

In June 2023, Nigeria passed the Nigerian Data Protection Act (NDPA) — the first full national law protecting your digital data. It sets clear obligations for companies and gives consumers stronger rights over how their information is handled.

What NDPA says in simple terms:

- Companies must get your consent before collecting your personal data.
- You have the right to know how your data is being used.
- You can ask a company to delete your data if you no longer want them to keep it.
- Companies must report to regulators if their data is hacked or leaked.

Under NDPA, businesses must obtain consent before collecting data, explain how it is used, delete it upon request, and report breaches to regulators. These simple but powerful rules shift control back to consumers, making the law a cornerstone of digital rights in Nigeria.

Mini Case Study – Bank Verification Number (BVN): Before NDPA, many fintech apps requested BVNs from users without explaining the purpose. Under NDPA, they must state clearly why they need your BVN, how it will be stored, and how long they will keep it.

4.2 Your Digital Rights as a Nigerian Consumer

The Nigerian Data Protection Act (NDPA 2023) gives every consumer clear control over their personal data. These rights ensure that individuals are not powerless in the face of data misuse.

Here are the key rights you now have under NDPA and related regulations:

The NDPA 2023 gives Nigerians a stronger voice in how their data is handled. These rights ensure that individuals are no longer passive subjects of data collection but active owners of their digital identity.

1. **Right to Consent:** Nobody should collect your data without your permission.
2. **Right to Access:** You can request to see the data a company holds about you.
3. **Right to Correction:** If your data is wrong (e.g., misspelled name, wrong age), you can demand corrections.
4. **Right to erasure ("Right to be Forgotten"):** You can ask for your data to be deleted when it is no longer needed.
5. **Right to Complain & Seek Redress:** If your data is misused, you can report to regulators.

With rights to consent, access, correction, erasure, and redress, Nigerian consumers now have legal tools to hold companies accountable for their actions. The challenge is awareness — these protections only work when people are aware of them and demand their enforcement.

Mini Case Study – SIM Card Registration: Nigerians were once required to register their SIM cards multiple times, providing NIN and BVN details. Under NDPA, telecom companies are expected to store your details securely and not expose you to repeated data risks.

4.3 Key Regulators Protecting You

Protecting digital consumers in Nigeria is a shared responsibility, and several government agencies play vital roles in enforcing laws and safeguarding data, as shown in Table 2.

Several government bodies enforce consumer digital rights in Nigeria:

- **Nigeria Data Protection Commission (NDPC):** The main body set up in 2023 to enforce NDPA.
- **National Information Technology Development Agency (NITDA):** Before NDPA, NITDA fined companies for data breaches.

- **Nigerian Communications Commission (NCC):** Protects telecom subscribers against fraud, unfair billing, and SIM misuse.
- **Central Bank of Nigeria (CBN):** Regulates how banks and fintechs handle your financial data.

Table 2: Key Regulators Protecting Consumers

Regulator	Role
NDPC	Enforces NDPA, ensures consumer data protection
NCC	Handles telecom fraud, SIM misuse, and billing complaints
NITDA	Tech regulation, data privacy enforcement
CBN	Oversees banks & fintechs, financial data protection
FCCPC	General consumer protection, including digital abuse
EFCC	Investigates cybercrime and fraud

The NDPC leads on data protection, NITDA addresses breaches, NCC secures telecom users, and the CBN oversees financial data practices. Together, these regulators form the backbone of digital consumer protection — but their effectiveness depends on citizens knowing where to turn when rights are violated.

Mini Case Study – NITDA Fine on Loan Apps (2022): NITDA fined a popular loan app ₦10 million for harassing Nigerians by sending debt-shaming messages to their contacts. This case, as illustrated below in

Figure 5, showed that digital abuse is punishable and that Nigerians have channels to fight back.

(a) High interest rate (b) reporting the loan app to regulators

(c) The regulator punishes the loan company

Figure 5: illustration of the case study above

4.4 Challenges with Enforcement in Nigeria

Even with strong laws in place, enforcing digital rights in Nigeria remains a challenge. Gaps in awareness, compliance, and oversight weaken consumer protection.

While the laws exist, the challenges are:

Strong laws are only effective when they are understood, respected, and enforced. In Nigeria, gaps in awareness, compliance, and oversight still weaken digital consumer protection.

- Many Nigerians are unaware of their rights.
- Companies often ignore the rules, betting that consumers will not report.
- Regulators lack enough human resources to monitor every digital company.

Many Nigerians remain unaware of their rights, and some companies capitalize on this ignorance. Consequently, regulators are overstretched in monitoring violations. Bridging these gaps requires a mix of public awareness, corporate responsibility, and stronger institutional capacity.

When citizens are unaware of their rights, companies exploit loopholes, and regulators are overstretched, data abuse goes unchecked. Closing this gap requires both stronger institutions and more informed consumers.

Mini Case Study – Data Breaches by Nigerian Banks: A leaked report in 2022 revealed that customer data from some Nigerian banks was being sold on WhatsApp groups. Many victims were unaware that they could demand accountability under Nigerian law.

4.5 Summary for Consumers

To simplify, here are the key truths every Nigerian digital consumer must remember:

- Your personal data belongs to you, not the company collecting it.
- NDPA 2023 gives you rights: consent, access, correction, deletion, and redress.
- Regulators like NDPC, NCC, NITDA, and CBN exist to protect you, as shown in Figure 6.

- Enforcement is still growing, but awareness is your first line of defense.

Figure 6: Regulators in Nigeria

Your data is yours, the law protects it, regulators exist to defend it, but awareness is your strongest safeguard. Stay informed, stay alert, and stay protected.

☞ If someone misuses your data, you now have legal backing to act**.**

4.6 Summary: Protecting Personal Data & Consumer Rights in Nigeria

Your personal data belongs to you, not the companies collecting it. The NDPA 2023 grants you fundamental rights, including consent, access, correction, deletion, and redress. Regulatory bodies like NDPC, NCC, NITDA, and CBN exist to protect you, though enforcement is still developing. Awareness of these rights represents your first line of defense—if someone misuses your data, you now have legal backing to act.

CHAPTER 5

Tools for Digital Self-Defense

Authors/Contributors: *A. A. Sadiq; T. A. Folorunso; B. A. Salihu*

Summary: Building Everyday Digital Resilience

Digital self-defense is about building protective habits before problems occur. The tools outlined—two-factor authentication, password managers, permission controls, and safe browsing practices—form a comprehensive defense system that any Nigerian can implement. With these tools, you can take personal control of your digital safety instead of waiting for regulators alone. Remember: your security is ultimately in your hands.

CHAPTER 5

Tools for Digital Self-Defense

5.1 Why Personal Digital Safety Matters

Staying safe online goes beyond relying on government regulations or company promises. True protection begins with personal habits and practical tools that strengthen your digital defenses. Just as you lock your doors at night, securing your accounts, devices, and data has become an everyday necessity in Nigeria's rapidly growing digital landscape.

Digital safety is not only about laws — it is also about what you do every day. Think of these tools like a "seatbelt" in your digital life. They do not stop accidents from happening, but they protect you when things go wrong.

5.2 Core Digital Safety Tools: Step-by-Step Guides

5.2.1 Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) means adding a second layer of security beyond your password. Even if scammers know your password, they cannot log in without your 2FA code. Thus, technology provides us with convenience — including instant banking, shopping, chatting, and entertainment. However, it also opens doors for hackers, scammers, and apps that misuse our data. The good news? You do not have to be an expert to protect yourself. Below **are** simple, step-by-step tools **every** Nigerian consumer can use.

- **How to use it (Google Authenticator example):**

  Two-Factor Authentication (2FA) adds an extra layer of security to your accounts, making it much harder for scammers to break in even if they know your password. Setting it up takes just a few steps.

To secure your accounts with Two-Factor Authentication (2FA), follow these simple steps:

1. Download Google Authenticator from the Play Store/App Store.
2. Open your app or banking platform settings → Look for Security or 2FA.
3. Choose "Use Authenticator App" (sometimes called OTP App).
4. Scan the QR code shown on your screen with the Authenticator app.
5. A 6-digit code will appear → enter it into the website/app.
6. Done! Now each time you log in, your Authenticator will generate a fresh code.

By enabling 2FA with an authenticator app, you lock your accounts with a unique, ever-changing code that only you can generate. This simple habit has already saved many Nigerians from falling victim to fraud. It is one of the most effective defenses against online attacks.

- **Nigerian Example:**

Two-Factor Authentication is not just a theory — Nigerian banks and consumers are already proving its value in real-life situations.

- GTBank, Zenith, and Opay now strongly encourage or require 2FA for sensitive transactions.
- Most Nigerian banks now use soft tokens (e.g., GTBank Token App, Access Bank SafeToken). Install, link it to your account, and generate one-time codes for transactions.
- In 2022, a Lagos student avoided ₦200,000 fraud when hackers guessed her Gmail password but were blocked by her 2FA code.

With banks like GTBank, Zenith, and Opay pushing 2FA through tokens and authenticator apps, Nigerians are better shielded from fraud. A Lagos student who avoided losing ₦200,000 thanks to 2FA

shows how this simple step can make the difference between safety and disaster.

👉 Always enable 2FA on social media (WhatsApp, Facebook, Instagram, Twitter), banking apps, and email accounts.

💡 **Mini Case Study – SIM Swap Fraud:** A Lagos businessman lost ₦3.2 **million after scammers swapped his SIM and reset his bank password. If he had enabled bank token and Authenticator, the thieves would not have been able to complete** the transfer.

🔑 5.2.2 Password Managers

Many Nigerians use the same password (such as 12345 or their phone number) across various platforms, including Facebook, email, and bank apps. This is dangerous — if one account is hacked, all are at risk. Black hackers love this. A password manager creates and remembers strong passwords for you, as illustrated in Figure 7. Many Nigerians reuse one password. A password manager stores strong, unique passwords for you.

Managing multiple strong passwords can be overwhelming, and reusing the same one across apps is risky. A password manager solves this problem by securely storing and generating unique logins for every account.

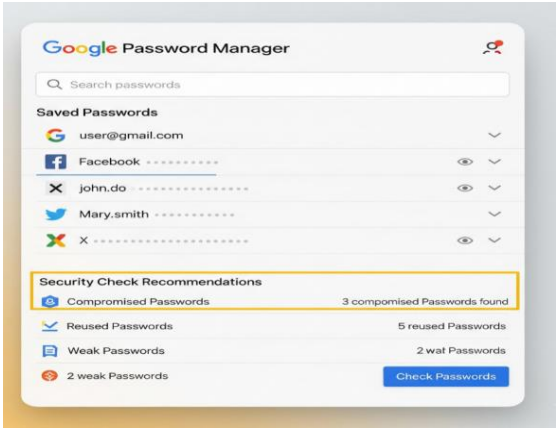


Figure 7: The interface of a Google password manager

To keep all your 9 safe, here is how to set up and use a password manager:

- **How to use it:**

1. Install a trusted manager like (e.g., Bitwarden, 1Password, LastPass, NordPass); some free versions exist.
2. Create one strong "master password" (write it down in a safe place).
3. Each time you log in somewhere, let the manager create a random, strong password.
4. Next time, it autofills for you — no need to memorize.
5. Use autofill to log in to sites without having to remember your credentials.

A password manager saves and generates strong, unique passwords for every account. With just one master password, you stay secure without the stress of memorizing them all.

By installing a trusted manager, creating one strong master password, and letting the app handle the rest, you eliminate weak or repeated passwords. This simple tool makes your digital life both safer and easier, ensuring that even if one account is compromised, the rest remain secure.

Mini Case Study – JAMB 2022 Hack:

- Several students' JAMB profiles were hijacked because they used simple, repeated passwords ("123456" or their names). With a password manager, each account could have had different, stronger passwords.
- In 2023, a fintech startup in Abuja suffered a breach. Customers who reused their Opay passwords on other apps were more exposed. Those with managers had unique passwords and stayed safe.

5.2.3 App Permission Settings (Android/iOS)

Every app you install asks for permissions (camera, contacts, microphone, location). Many Nigerians press "Allow All," which can expose private data. Apps often request more data than they need — a

calculator app asking for microphone access, or a game asking for your contacts.

- **How to manage it (Android example):**

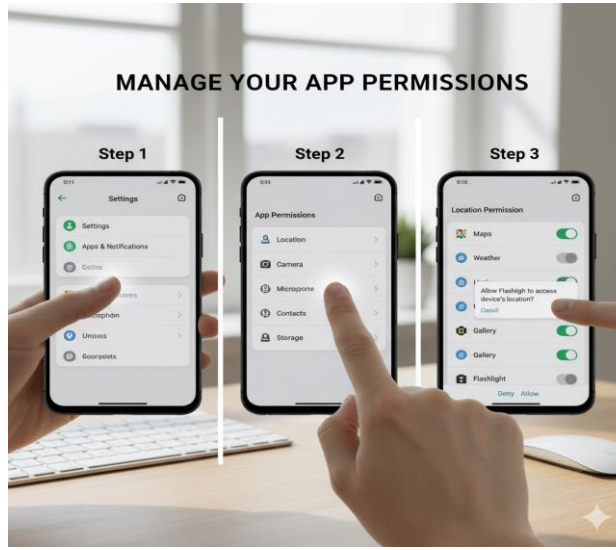


Figure 8: App permission process on an Android Device

1. Open Settings → Apps & Notifications → App Permissions (as demonstrated in Figure 8 above).
2. Check permissions by category (Location, Camera, Contacts, etc.).
3. If an app does not need it, turn it off.

- **On iPhone (iOS):**

1. Go to Settings → Privacy & Security (as demonstrated in Figure 9).
2. Tap the permission (e.g., Camera, Microphone).
3. Switch off apps that do not need it.

Figure 9: App permission process on an iOS Device

- **Real Example:**
- In Nigeria, several flashlight apps were found to be harvesting user contacts for spam. A student in Minna discovered her location was being tracked unnecessarily by a free game until she disabled permissions.

☞ ***Golden Rule:*** If an app does not need access, deny it.

Mini Case Study – Loan Apps in Nigeria: Some loan apps were caught harassing borrowers by accessing their contacts and photos. If users had blocked contact access in settings, the apps could not have messaged family and friends.

5.3 Safe Use of Public Wi-Fi & Social Media

Public Wi-Fi (found in cafés, airports, and campuses) is convenient but often unsafe. Hackers can spy on your traffic. Free Wi-Fi at airports, universities, or restaurants can be traps — hackers may intercept your data.

5.3.1 How to stay safe:

- Avoid banking or shopping on free Wi-Fi.
- Use VPN apps (like ProtonVPN, TunnelBear) for encrypted browsing.

- Switch off Wi-Fi auto-connect.

5.3.2 Social Media Safety Steps

Social media connects friends, businesses, and communities — but it also creates openings for scammers. Staying safe means being intentional about what you share and with whom you interact.

When it comes to social media, protect yourself by following these simple rules:

- Avoid oversharing (posting travel plans, account screenshots, or sensitive details).
- Be wary of "free giveaways" asking for BVN or card numbers.
- Verify friend requests — many are impersonation scams.
- Do not overshare (avoid posting your travel plans, ID cards, or bank alerts).
- Always double-check friend requests — scammers create fake profiles.
- Review your privacy settings on Facebook, Instagram, Twitter/X.

By avoiding oversharing, ignoring suspicious giveaways, verifying requests, and tightening privacy settings, you make yourself a harder target for fraud and impersonation. Smart posting is not just about image — it is about protecting your data, your money, and your identity.

5.3.3 Wi-Fi Safety Steps:

Public Wi-Fi may be convenient, but it is one of the easiest ways for hackers to steal personal data. Simple precautions can keep your online activity safe, as shown in Figure 10.

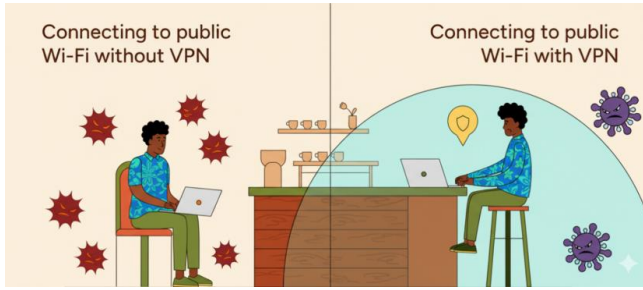


Figure 10: Why you should avoid using public Wi-Fi for banking or sensitive logins

1. Avoid using public Wi-Fi for banking or sensitive logins.
2. Use a VPN app (e.g., NordVPN, ProtonVPN, TunnelBear) for protection.
3. Always log out after use.
4. By avoiding sensitive logins on public Wi-Fi, using a VPN for encryption, and always logging out after use, you protect yourself from common cyberattacks, some of the risks are shown in Figure 11. A little caution goes a long way in keeping your data secure.
5. **Figure 11:** Risks of connecting to a public Wi-Fi

5.3.4 Nigerian Case:

Mini Case Study – Facebook Kidnap Scam:

- A university student in Abuja posted her travel details on Facebook. Scammers used the info to trick her family with fake kidnap calls. Limiting what she shared could have prevented this from happening.
- In 2022, scammers at the UNILAG campus used free Wi-Fi to steal student logins. Victims lost access to emails and even bank alerts.

☑ Quick Checklist for Everyday Safety

Here is a one-minute safety checklist (as seen in Table 3) for every Nigerian digital consumer:

- Enable 2FA on all major apps (email, social media, banking).
- Use a password manager instead of reusing passwords.
- Regularly check app permissions (deny unnecessary ones).
- Be cautious on public Wi-Fi — use VPN or avoid banking.
- Think before you share on social media.
- Keep your phone updated with the latest security patches.
- Report suspicious activity to NCC, NDPC, or your bank immediately.

Table 3: Everyday Digital Safety Checklist

Action	Done ✓
Enable 2FA on all major apps.	☐
Use a password manager.	☐
Review app permissions regularly.	☐
Avoid banking on public Wi-Fi.	☐
Keep phone software updated.	☐
Report fraud immediately	☐

With these tools, Nigerians can take personal control of their digital safety — instead of waiting for regulators alone.

5.4 Summary: Building Everyday Digital Resilience

Digital self-defense is about building protective habits before problems occur. The tools outlined—two-factor authentication, password managers, permission controls, and safe browsing practices—form a comprehensive defense system that any Nigerian can implement to protect themselves. With these tools, you can take personal control of your digital safety instead of waiting for regulators alone. Remember: your security is ultimately in your hands.

CHAPTER 6

Digital Rights for Students & Youth

Authors/Contributors: *T. A. Folorunso; U. S. Dauda; A. O. Abdulbaki; T. A. Mamman*

Summary: Empowering the Digital Generation

Nigerian students are not just consumers of digital technology—they are shapers of the digital future. By defending their rights, building digital literacy clubs, and educating peers, youth can ensure the internet remains a tool of empowerment rather than exploitation. The power to change Nigeria's digital landscape lies with informed, organized, and active young people who understand their rights and are willing to teach others.

CHAPTER 6

Digital Rights for Students & Youth

5.5 Understanding Digital Rights

Across campuses and communities, young Nigerians are some of the most active digital citizens — learning, creating, and connecting online every day. Nevertheless, with this opportunity comes new risks: surveillance, misinformation, and exploitation. Recognizing digital rights is therefore not just a legal issue but a practical necessity for safeguarding the future of education, innovation, and free expression.

The internet is more than entertainment — it is a space for learning, organizing, and innovation. For Nigerian students and youth, digital rights are as important as access to electricity or education. Yet, many are unaware of what these rights mean, how they are threatened, and how they can be protected.

6.1.1 Why Digital Rights Matter in Nigeria

Digital rights are human rights applied in the online world — freedom of expression, access to information, privacy, and protection from harassment.

Why it matters:

Digital rights are not abstract — they shape how students and young people in Nigeria access knowledge, express themselves, and protect their privacy online.

- **Access & Inequality:** Many Nigerian students depend on campus Wi-Fi, cybercafés, or shared devices. Limiting access or making the internet unaffordable cuts off opportunities.
- **Surveillance & Privacy:** Young people often use social media without realizing their data is being tracked, sold, or misused.

- **Freedom of Expression:** Nigeria has witnessed instances where tweets or posts have led to arrests or intimidation. Students must be aware of their boundaries and protections.

Limited access deepens inequality, unchecked surveillance threatens privacy, and restrictions on expression put youth at risk. For Nigerian students, defending digital rights is about safeguarding opportunities, safety, and freedom in the online world.

Mini Case: In 2021, during the Twitter ban in Nigeria, many student groups were unable to run campaigns, share research, or even promote small businesses online. Those with VPNs continued, but the event highlighted the fragility of digital rights.

👉 For youth, digital rights are not abstract. They affect scholarships, job opportunities, campus activism, and even personal safety.

5.6 Building Campus Awareness

6.2.1 Building Digital Literacy Clubs on Campus

A strong way to safeguard rights is through collective knowledge. Students can form clubs that build awareness and teach practical skills.

Steps to start a Digital Literacy Club

Starting a Digital Literacy Club on campus is a practical way for students to build awareness and protect one another. Here is how to get started:

1. **Gather a small group** of interested students (ICT, law, mass communication, social sciences).
2. **Agree on focus areas**: e.g., online privacy, cyber safety, misinformation, or Advocacy.
3. **Get campus support** from the Student Union Government (SUG), faculty, or ICT departments.
4. **Run activities**:
    - "Digital Hygiene Day" (checking passwords, app permissions, 2FA).
    - Workshops on fact-checking and identifying fake news.

- Invite guest speakers from NGOs like Paradigm Initiative, Enough is Enough (EiE), or tech startups.

5. **Document and share**: publish short guides, podcasts, or blogs for other students.

By forming groups, selecting focus areas, securing faculty support, organizing activities, and sharing knowledge, students can cultivate a campus-wide culture of digital safety. These clubs empower young people to become leaders in protecting their rights and promoting digital literacy.

Mini Case: At FUT Minna, a student group once organized a WhatsApp seminar on **"Protecting Your Digital Footprints"** with over 200 participants. Students who attended later taught their classmates how to spot phishing links.

☞ A club does not have to be big — it just has to be consistent.

5.7 Advocacy and Peer Education

📢 6.3.1 Advocacy and Peer Education

In today's digital world, young Nigerians are not only the largest group of internet users but also the most vulnerable to online risks. This makes their role in shaping digital rights even more important. Advocacy is not limited to lawyers or policymakers — students and young people can play a direct role in building awareness, promoting safe practices, and holding institutions accountable. By leveraging their creativity, energy, and networks, they can spark real change on campuses, online platforms, and within their communities.

Ways to Advocate
Students and youth can push digital rights forward in powerful ways, including:

- **Peer Training:** Teach classmates how to set up 2FA, detect scams, or manage digital stress.

- **Campaigns:** Use Instagram, TikTok, or campus radio to spread digital rights messages.
- **Dialogue with Authorities:** Engage with student leaders, ICT directors, or lecturers to integrate digital literacy into orientation programs.
- **Partner with NGOs:** Groups like Paradigm Initiative (PIN) run the *Digital Rights Academy* — students can join and later train others.

By training peers, running awareness campaigns, engaging school authorities, and partnering with NGOs, students can transform knowledge into collective action. When youth lead the way, digital rights become a shared culture, not just a policy on paper.

Mini Case: In Enugu, students launched the "#SafeSurfNaija" campaign. They used skits and memes on TikTok to show how scammers trick people. The campaign reached over 10,000 young Nigerians online.

☞ Advocacy is not just about protesting; it is about teaching, creating, and sharing knowledge.

☑ 6.3.2 Quick Action Plan for Students

✓ Learn your digital rights (privacy, freedom of expression, access).
✓ Join or start a digital literacy club on campus.
✓ Run peer-to-peer sessions (online or offline).
✓ Use social media positively for campaigns.
✓ Collaborate with NGOs and tech hubs.

📌 Takeaway:
Nigerian students are not just consumers of digital technology — they are shapers of the digital future. By defending their rights, forming clubs, and educating their peers, young people can help ensure that the internet remains a tool of empowerment rather than exploitation.

5.8 Summary: Empowering the Digital Generation

Nigerian students are not just consumers of digital technology—they are shapers of the digital future. By defending their rights, building digital literacy clubs, and educating peers, youth can ensure the internet remains a tool of empowerment rather than exploitation. The power to change Nigeria's digital landscape lies with informed, organized, and active young people who understand their rights and are willing to teach others.

CHAPTER 7

Future of AI & Governance in Nigeria

Authors/Contributors: *S. Zubair; J. A. Bala; T. A. Folorunso; A. A. Sadiq*

Summary: Shaping an Inclusive AI Future

AI will shape the future of jobs, education, and governance in Nigeria. Students and youth must be not only users of AI but also critics, innovators, and watchdogs—ensuring technology serves people, not just profits. The decisions made today about AI governance will determine whether artificial intelligence becomes a tool for empowerment or exploitation. Young people have a crucial role in shaping these conversations for an inclusive, transparent, and accountable AI future.

CHAPTER 7

Future of AI & Governance in Nigeria

5.9 Understanding AI and Its Impact

Nigeria's digital future will be shaped not only by how people use technology but also by how it is governed. Artificial Intelligence promises efficiency and innovation, yet it also raises deep questions about ethics, fairness, and accountability. As the country embraces AI in finance, education, and public services, building clear rules and safeguards will determine whether these tools empower citizens or exploit them.

Artificial Intelligence (AI) is no longer science fiction. From chatbots that help with banking to face recognition at airports, AI is shaping how Nigerians work, learn, and interact. But as AI grows, so does the debate: Who controls it? Who benefits from it? Who is held responsible when it goes wrong?

This section introduces young Nigerians to the debates surrounding AI governance — the rules, ethics, and responsibilities associated with using AI in society.

5.10 Explainable AI: Why Transparency Matters

🔍 7.2.1 Should AI Models Be Explainable?

Artificial Intelligence often works like a "black box," producing decisions without showing how they were made. This lack of transparency becomes a serious issue when AI is utilized in sensitive areas, such as banking, hiring, or security. For example:

- A bank's loan approval AI rejects a student's application without explanation.
- A recruitment platform ranks candidates using hidden algorithms.

- A facial recognition system misidentifies people with darker skin tones.

Unexplainable AI risks unfair rejections, biased rankings, and misidentifications that consumers cannot challenge. For Nigerians, explainability is crucial to ensure that AI systems are fair, trustworthy, and accountable to the people they impact.

7.2.2 Why explainability matters in Nigeria:
For AI to truly benefit Nigerians, its decisions must be open to scrutiny. Explainability is not a luxury — it is a safeguard that ensures technology serves people fairly and responsibly.

- **Fairness:** Students and job seekers need to know *why* they were rejected.
- **Trust:** Citizens must trust that systems are not biased.
- **Accountability:** Without explanations, companies and government agencies can avoid responsibility.

Transparent AI promotes fairness for students and job seekers, builds trust among citizens, and holds institutions accountable. Without it, algorithms become tools of exclusion and abuse rather than empowerment.

☞ **In short:** AI must be explainable so that ordinary Nigerians can challenge wrong or unfair decisions.

5.11 Balancing Regulation and Innovation

⚖ 7.3.1 Balancing Regulation vs. Innovation

Nigeria is Africa's largest tech hub, with thousands of startups working in fintech, agritech, and health. Strict laws might slow innovation — but no laws at all could leave citizens vulnerable.

The balancing act:

- **Too much regulation** → discourages startups and scares investors.

- **Too little regulation** → opens the door to fraud, privacy violations, and unsafe AI.

7.2.3 Possible Nigerian approach

To balance innovation with consumer protection in Nigeria's AI future, three approaches stand out:

1. **Regulatory Sandboxes:** Safe spaces where startups can test AI under light supervision.
2. **Sector-based guidelines:** For health, banking, education — instead of one-size-fits-all rules.
3. **Youth input:** Student unions, innovation hubs, and tech clubs should be consulted on AI policies.

With sandboxes for testing, sector-specific rules, and youth participation, Nigeria can regulate AI wisely — protecting citizens without stifling creativity.

Mini Case: The Central Bank of Nigeria (CBN) once banned cryptocurrency, but young innovators moved to peer-to-peer systems. This suggests that over-regulation does not hinder innovation — it merely drives it underground.

👉 Nigeria must strike a balance: protect citizens without killing creativity**.**

5.12 Multi-Stakeholder Governance

🏛 7.3.1 The Role of NCC, NITDA, and Civil Society

AI governance will not succeed if left only to the government. It requires multi-stakeholder involvement.

- **NCC (Nigerian Communications Commission):** Ensures telecom companies use AI responsibly, especially in data privacy and customer protection.
- **NITDA (National Information Technology Development Agency):** Drafts national AI policies, guidelines, and supports local innovation.

- **Civil Society & Youth Groups:** Watchdogs that ensure laws respect human rights, raise awareness, and hold both government and companies accountable.

Mini Case:
In 2023, NITDA released a draft National AI Strategy, which included public consultations. Civil society groups, such as Paradigm Initiative, pushed for stronger language on data privacy and the inclusion of rural communities.

☞ The future will depend on collaboration: government sets the rules, companies build solutions, and civil society ensures fairness.

☑ 7.3.2 Quick Reflection for Students

✓ Ask: If an AI decides for me, can I appeal it?
✓ Support policies that balance innovation and protection.
✓ Engage in campus debates on AI ethics — the voices of young Nigerians matter.
✓ Follow updates from **NCC** and **NITDA** to stay informed.
✓ Join civil society campaigns to defend digital rights in the AI era.

📌 Takeaway:

AI will shape the future of jobs, education, and governance in Nigeria. Students and youth must not only be users of AI but also critics, innovators, and watchdogs — ensuring technology serves the people, not just profits.

5.13 Summary: Shaping an Inclusive AI Future

AI will shape the future of jobs, education, and governance in Nigeria. Students and youth must not only be users of AI but also critics, innovators, and watchdogs—ensuring that technology serves people, not just profits. The decisions made today about AI governance will determine whether artificial intelligence becomes a tool for empowerment or exploitation. Young people have a crucial role in shaping these conversations for an inclusive, transparent, and accountable AI future.

CHAPTER 8

Call to Action

Authors/Contributors: *A. U. Usman; A. O. Alenoghena; B. A. Salihu; M. David; U. S. Dauda*

Summary: Becoming a Digital Protector

The digital economy offers tremendous opportunities for Nigerian youth, but also presents significant risks. By following the 10 Commandments of Digital Consumer Protection, knowing where to report problems, and staying informed about your rights, you become not just a consumer but a protector of the digital commons. Your digital protection journey starts now—with the next choice you make online. Remember: every person you teach and every right you exercise makes Nigeria's digital space safer for everyone

CHAPTER 8

Call to Action

5.14 Taking Personal Responsibility

The future of Nigeria's digital space will not be secured by laws alone but by how individuals choose to act each day. Every click, every password, and every online interaction shapes whether the internet becomes a tool for empowerment or exploitation. For students, young people, and everyday consumers, digital protection starts with awareness and consistent habits that safeguard identities, finances, and reputations.

Digital consumer protection is not just about laws — it is about everyday choices we make online. Students and young Nigerians are the first line of defense against scams, data theft, and online exploitation.

5.15 The 10 Commandments of Digital Consumer Protection

To stay safe, follow the "***10 Commandments***" of digital consumer protection:

Digital safety in Nigeria goes beyond avoiding fraud — it requires daily habits that protect your identity, money, and dignity. The "10 Commandments of Digital Consumer Protection" provide a simple but powerful code of conduct, combining safe practices with shared responsibility so that individuals and communities can thrive securely online.

- The 10 Commandments of Digital Consumer Protection

1. **Thou shalt use strong, unique passwords** (never the same one for bank, email, and social media).
2. **Thou shalt enable 2FA** on all important accounts (banking, Gmail, WhatsApp, Instagram).
3. **Thou shalt not click suspicious links** in emails, SMS, or WhatsApp groups — even if from "friends."
4. **Thou shalt not overshare personal details** (phone number, address, BVN) on social media.

5. **Thou shalt always review app permissions** (deny apps access to your camera, mic, or location if unnecessary).
6. **Thou shalt avoid public Wi-Fi for banking or sensitive transactions.**
7. **Thou shalt double-check before sending money online** — verify seller, account name, and reviews.
8. **Thou shalt report fraud immediately** to banks, NCC, or consumer protection agencies.
9. **Thou shalt educate peers** — share safety tips in WhatsApp groups, student clubs, and on campus.
10. **Thou shalt stay updated** — cybercriminals change tactics daily; continuous learning is protection.

☞ **Memorize these rules. Share them. Live by them**.

These commandments are not just tips but a culture of awareness. From strong passwords and 2FA to careful sharing, fraud reporting, and peer education, they equip Nigerians to resist scams and data misuse. By adopting them and remaining vigilant as cybercriminals evolve, digital consumers can help build a safer, more resilient online future for themselves and others.

5.16 ☎ Resources & Hotlines for Complaints / Reporting Fraud in Nigeria

When faced with fraud, scams, or data breaches, knowing where to report is just as important as prevention. In Nigeria, several reputable agencies offer direct channels for assistance and redress.

If you suspect fraud, data breach, or online scams, here are trusted places to report:

- **NCC (Nigerian Communications Commission):**
  • Toll-Free Number: **622** (for telecom complaints: over-billing, unsolicited SMS, fraud).
- **CBN / Banks:**
  • Call your bank's fraud desk immediately.

• Use the **NIBSS "Nigerian Bank Account Verification" portal** to confirm account names.

- **EFCC (Economic and Financial Crimes Commission):**
  • Report cybercrime via efccnigeria.org
  • Hotlines vary by zone, but Lagos Zonal Office: **+234 818 975 1701**
- **NITDA (National Information Technology Development Agency):**
  • Email: **info@nitda.gov.ng** (for data privacy breaches).
- **Consumer Protection Council (FCCPC):**
  • Hotline: **0805 600 2020**
  • Website: fccpc.gov.ng
- **Police Cybercrime Unit:**
  • Report at any state CID or via **interpolnigeria@npf.gov.ng**

From NCC's toll-free line for telecom complaints to banks' fraud desks, EFCC, NITDA, FCCPC, and the Police Cybercrime Unit, Nigerians have multiple avenues to seek protection. Quick reporting not only safeguards your money and data but also helps regulators track and shut down fraudsters. Awareness of these hotlines is a vital tool in every consumer's digital defense.

📌**Final Note to Students & Youth:** Digital safety is not someone else's job. **You are your own first defense.** Protect your data, protect your money, and protect your future. When in doubt — **pause, verify, and report.**

5.17 Summary: Becoming a Digital Protector

The digital economy offers tremendous opportunities for Nigerian youth, but also presents significant risks. By following the 10 Commandments of Digital Consumer Protection, knowing where to report problems, and staying informed about your rights, you become not just a consumer but a protector of the digital commons. Your digital protection journey starts now—with the next choice you make online. Remember: every person you teach and every right you exercise makes Nigeria's digital space safer for everyone.

CHAPTER 9

Further Reading

Authors/Contributors: *A. A. Sadiq; M. David; J. A. Bala*

Summary: Key Resources for Digital Consumer Protection

Herein, essential resources for understanding digital consumer protection, including Nigerian regulations, international guidelines, academic research, and case studies are highlighted. Nigerian frameworks such as FCCPC guidelines, NDPR, CBN consumer protections, and NCC codes safeguard rights across sectors. Internationally, OECD, UNCTAD, EU GDPR, and World Bank reports provide best practices and global benchmarks. Academic works examine ethical AI use, data monetization, and consumer profiling risks, while case studies illustrate challenges like AI bias, predatory lending, facial recognition bias, and telecom fraud. Collectively, these resources provide a comprehensive foundation for promoting safe, fair, and ethical digital consumer practices.

CHAPTER 9

Further Reading

To deepen your understanding of digital consumer protection, the following resources provide useful insights. They include Nigerian regulatory frameworks, international guidelines, academic works, and global case studies. First, an outline of each is provided, categorized under either Nigerian or international guidelines.

9.1 Nigerian Regulatory and Policy Documents

9.1.1 ***FCCPC Consumer Protection Frameworks and Guidelines*** – Outlines consumer rights, complaint channels, and enforcement mechanisms in Nigeria. Accessed via: https://fccpc.gov.ng/resources-library/regulations/

9.1.2 ***Nigerian Data Protection Regulation (NDPR, 2019)*** – The country's primary data privacy regulation issued by NITDA. *Accessed via:* https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf

9.1.3 ***Central Bank of Nigeria (CBN) Consumer Protection Framework*** – Focuses on safeguarding consumer interests in financial services. Accessed via: https://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20(final).pdf

9.1.4 ***Nigerian Communications Commission (NCC) Consumer Code of Practice Regulations*** – Protects telecom subscribers against fraud, poor service, and exploitation. Accessed via: https://www.ncc.gov.ng/sites/default/files/2024-11/Documents/Draft%20-

%20Consumer%20Code%20of%20Practice%20Regulations.pdf

9.2 International Guidelines

9.2.1 **OECD (2016), Consumer Protection in E-commerce** – Provides international best practices for safeguarding online consumers. Accessed via: https://www.oecd.org/content/dam/oecd/en/publications/reports/2016/05/oecd-recommendation-of-the-council-on-consumer-protection-in-e-commerce_g1g66e4e/9789264255258-en.pdf

9.2.2 **UNCTAD, United Nations Guidelines for Consumer Protection** – A global reference framework for consumer rights in the digital economy. Accessed via: https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf

9.2.3 **European Union General Data Protection Regulation (GDPR, 2018)** – The most comprehensive global data protection framework. Accessed via: https://edpo.com/representative-services/data-act-legal-representative/?utm_source=google&utm_medium=cpc&utm_campaign=data_act&gad_source=1&gad_campaignid=22690686610&gclid=CjwKCAjwlOrFBhBaEiwAw4bYDSEv-bK4oLO_7KBqIzwwjWbRpI42_A7leztYL0om5cJbw7Y8cp3eDhoCrT0QAvD_BwE

9.2.4 **World Bank (2021), Digital Economy for Africa Report** – Explores opportunities and risks in Africa's emerging digital markets. Accessed via: https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/Digital-Economy-RepSudan-jun22.pdf

9.3 Academic and Research Sources

9.3.1 Taddeo & Floridi (2018), *How AI can be a force for good* – Discusses the ethical use of artificial intelligence.

9.3.2 Zuboff (2019), *The Age of Surveillance Capitalism* – Examines how companies monetize consumer data.

9.3.3 Helberger (2016), *profiling and targeting consumers in the Internet of Things* – Explores risks of data-driven consumer profiling.

9.4 **Case Studies and Reports**

9.4.1 **AI bias in credit scoring** – Analyses from Brookings Institution and the World Economic Forum on how algorithms can perpetuate discrimination.

9.4.2 **Loan app exploitation in Nigeria** – FCCPC investigations and press releases (2021–2023) on predatory lending practices.

9.4.3 **Facial recognition bias** – MIT Media Lab's *Gender Shades* study highlighting racial and gender bias in AI systems.

9.4.4 **Telecom fraud and SIM swap scams** – NCC consumer alerts on protecting mobile users.

References

1. Federal Competition and Consumer Protection Commission (FCCPC). (n.d.). Consumer Protection Frameworks and Guidelines. Abuja: FCCPC.
2. Nigerian Communications Commission (NCC). (n.d.). Consumer Code of Practice Regulations. Abuja: NCC.
3. Nigerian Data Protection Regulation (NDPR). (2019). Abuja: National Information Technology Development Agency (NITDA).
4. Central Bank of Nigeria (CBN). (2016). Consumer Protection Framework. Abuja: CBN.
5. Organisation for Economic Co-operation and Development (OECD). (2016). Consumer Protection in E-commerce. Paris: OECD Publishing.
6. United Nations Conference on Trade and Development (UNCTAD). (2016). United Nations Guidelines for Consumer Protection. Geneva: UNCTAD.
7. European Union. (2018). General Data Protection Regulation (GDPR). Brussels: EU.
8. World Bank. (2021). Digital Economy for Africa Report. Washington, DC: World Bank.
9. Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science and Engineering Ethics, 24(1), 1–6.
10. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.
11. Helberger, N. (2016). Profiling and targeting consumers in the Internet of Things. Journal of Consumer Policy, 39(4), 405–421.

12. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

13. Brookings Institution. (2020). Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms. Washington, DC: Brookings.

14. World Economic Forum (WEF). (2018). The ethics of artificial intelligence and machine learning. Geneva: WEF.

ABOUT THE NCC PROFESSORIAL CHAIR ENDOWMENT, FEDERAL UNIVERSITY OF TECHNOLOGY MINNA

Established in the year 2023.

Vision: To promote inventions and innovations that will propel ICT solutions.

Mission: To encourage effective research and development efforts by all communications industry practitioners in the field of Engineering, Computer Science, ICT, and Social Sciences.

WHAT WE DO

Research and Development

Facilitating research team meetings and brainstorming sessions to explore new concepts and architectures, encouraging active participation from postgraduate students and other team members.

Skills Development and Training

The endowment offers mentorship, hands-on training, and expert insights through workshops, symposiums, testbeds, and laboratories.

Dissemination And Knowledge Transfer

The endowment publishes research findings in reputable journals and presents them at international conferences. It also conducts workshops, webinars, and public lectures to share project outcomes.

Infrastructure Development

The endowment establishes specialized laboratories, testbeds, and experimental platforms to enhance practical implementations and testing.

Collaboration Partnership

The endowment forms partnerships with leading research institutions, tech companies, and industry stakeholders.

Policy Recommendations

The endowment collaborates with the government, regulators, and stakeholders to offer recommendations and funding for technological advancements.

Socio-Economic Impact Assessment

The endowment assesses the socioeconomic impacts of technologies and makes recommendations to ensure they benefit society and national development.

OUR TEAM

Engr. Professor Abraham U. Usman is a dedicated educator with over 25 years of teaching experience in Electrical and Electronics Engineering, He coordinates the NCC Professorial chair endowment. His research interests include Radio Propagation Modelling, Mobile Radio Resource Utilization, Antenna Design, and the Application of IoT and AI in Engineering. He has published widely in national and international journals and conferences.

Engr. Prof. Caroline O. Alenoghena, a Professor of Telecommunications Engineering, focuses her research on Artificial Intelligence applications in Wireless, Green, and Optical Communications, as well as Telemedicine. She leads the Advanced Engineering & Innovation Research Group (AEIRG) and initiated the FUTEC Business Incubation Hub, promoting the "ACADO-Preneurship" concept to turn academic research into viable businesses.

Engr. Dr. Michael David holds a Bachelor's, Master's, and PhD degree in Engineering. He is an Associate Professor at the Federal University of Technology, Minna, Nigeria. Dr. David has undergone CEFE training and is a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN). Additionally, he is a member of the Fiber Optic Association, Inc. in the USA. His research interests encompass several areas, including optical absorption sensors, mobility management in wireless communication, Li-Fi, Wi-Fi, IEEE 802.11, Wireless LAN, and Non-Orthogonal Multiple Access (NOMA).

Engr. Dr. Suleiman Zubair is an associate professor in the Department of Telecommunications Engineering. He holds a Bachelor's degree in Electrical and Computer Engineering, a Master's degree in Communication Engineering, and a PhD in Electrical Engineering. He is CEFE-trained and is registered with the Council for the Regulation of Engineering in Nigeria (COREN).

Engr. Dr. Bala Alhaji Salihu is an Associate Professor in the Telecommunications Engineering department at the Federal University of Technology, Minna, Nigeria. He holds a PhD from Beijing University of Posts and Telecommunications. His research specializes in Telecommunications, Mobile communications, and IoT technologies. Salihu has published widely and led FUT Minna students to victory in the Huawei 2024 and 2025 global ICT competition. he has earned accolades such as the Huawei Best ICT Lecturer of the Year (2019).

Innocent Chika holds a Bachelor's in Electronic and Computer Engineering and is pursuing a Master's degree at the Federal University of Technology Minna. He serves as a graduate assistant at the NCC Professorial Chair Endowment.

Abdulkadir O. Abdulbaki is a researcher and hold s Master's degree in Communication Engineering from the Federal University of Technology, Minna, Nigeria. He works as a Graduate Assistant at the NCC Professorial Chair Endowment.

Thomas Alhassan Mamman is a Telecommunications Engineering graduate with a bachelor's degree in the field. He is currently advancing his education by pursuing a Master's degree at the Federal University of Technology in Minna, Nigeria, where he also works as a Graduate Assistant in the Telecommunications Engineering department.