Regulating Consumer Data Protection in Kenya's Digital Credit Services: Assessing the Effectiveness of Informed Consent in Law

By

Jude Oundo

116302

Master of Laws

March 2025

Regulating Consumer Data Protection in Kenya's Digital Credit Services: Assessing the Effectiveness of Informed Consent in Law

By

Jude Oundo

Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Laws at Strathmore University

Strathmore Law School
Strathmore University
Nairobi, Kenya

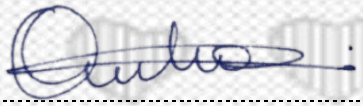
March 2025

DECLARATION AND APPROVAL

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Student's Name: **Jude Oundo** Date: **06th March 2025**

Students Signature: 

Approval

The LLM Thesis of Jude Oundo was reviewed and approved for examination by the following:

Dr. Japheth Odhiambo,
Strathmore Law School,
Strathmore University

Dr. Jane Wathuta,
Dean, Strathmore Law School,
Strathmore University

Dr. Bernard Shibwabo,
Director of Graduate Studies,
Strathmore University

ABSTRACT

Kenya's rapid expansion of Digital Credit Services (DCS) has significantly improved financial inclusion, especially for unbanked and underbanked populations. However, this growth has raised serious concerns about consumer data protection due to the vast amounts of personal and financial information collected by Digital Credit Providers (DCPs). This study examines the effectiveness of the informed consent model within Kenya's legal and regulatory framework in ensuring consumer data privacy in digital lending. Despite the existing regulatory framework, major gaps remain in protecting consumers' rights and ensuring they fully understand how their data is collected, processed, and shared.

The study first explores the development of Digital Financial Services (DFS) in Kenya, emphasizing how mobile money platforms and financial technology (FinTech) have facilitated the rise of digital lending. While these innovations have provided financial access to millions, they have also created data privacy vulnerabilities. Consumers often provide their data without adequate transparency or meaningful consent. Key concerns include information asymmetry, coercive consent mechanisms, algorithmic credit scoring opacity, and regulatory challenges surrounding artificial intelligence (AI) and big data applications.

To analyse these issues, the study evaluates various consent models, including informed consent, dynamic consent, opt-in and opt-out models, implied consent, and granular consent. It finds that Kenya's reliance on informed consent is inadequate because consumers often agree to data collection without fully understanding the implications. Factors such as complex terms and conditions, low digital literacy, and manipulative design strategies make it difficult for consumers to make rational, informed decisions about their data privacy. Cognitive biases and information overload further weaken the effectiveness of informed consent.

The study also reviews Kenya's legal and regulatory framework for consumer data protection in digital lending. While the existing laws provide a foundation, enforcement remains a challenge. The Office of the Data Protection Commissioner (ODPC) lacks the capacity to enforce regulations effectively, and there is insufficient coordination among key regulators like the Central Bank of Kenya (CBK) and the Communications Authority of Kenya (CAK). Additional gaps include unclear guidelines on AI-driven decision-making, weak penalties for data breaches, and a lack of consumer education initiatives.

To put Kenya's regulatory challenges into a global perspective, the study compares its consumer data protection framework with the European Union's General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA). The GDPR is found to be a strong model, ensuring that consent is freely given, specific, informed,

and unambiguous, with strict enforcement mechanisms. South Africa's approach aligns with GDPR principles but faces enforcement challenges similar to Kenya's, highlighting the difficulty of balancing innovation with consumer protection.

The study recommends several measures to enhance consumer data protection. These include adopting dynamic consent models, which allow users to modify data-sharing preferences over time; strengthening enforcement mechanisms through better regulatory coordination; increasing consumer awareness and financial literacy; implementing privacy-by-design principles in digital credit services; and fostering cross-border cooperation in regulating digital lending.

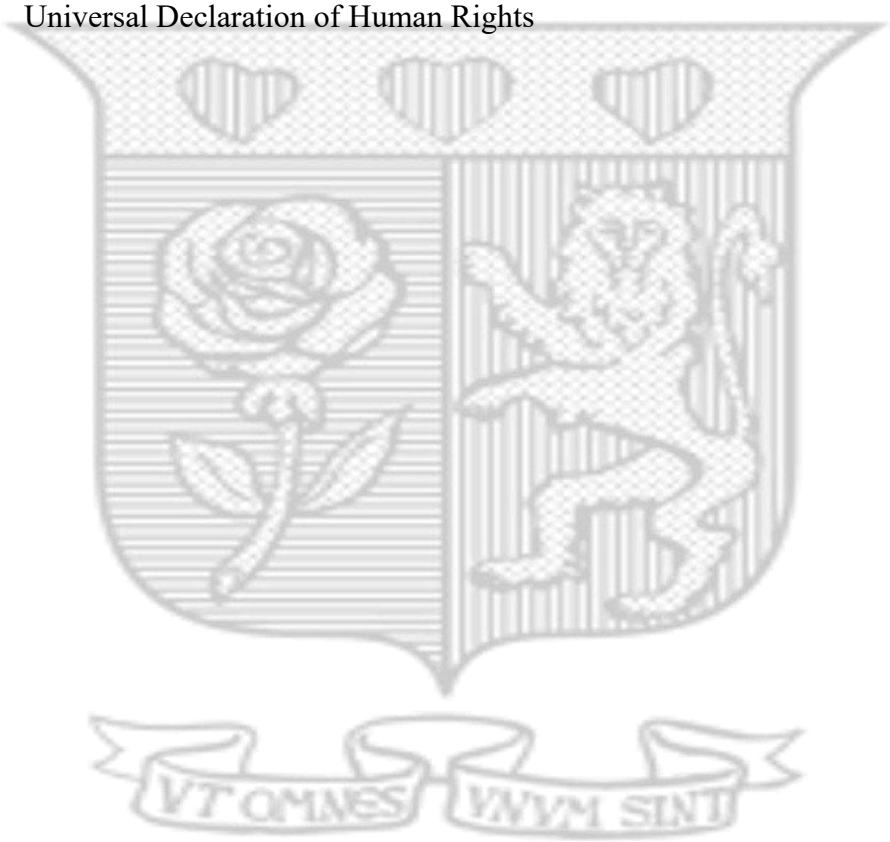
In conclusion, while Kenya has made progress in consumer data protection, its reliance on informed consent is inadequate in addressing risks associated with AI, big data, and algorithmic decision-making. A more adaptive and consumer-centric approach is needed, incorporating dynamic consent, stronger enforcement, and enhanced consumer education to ensure digital borrowers are protected from data exploitation. This study contributes to discussions on financial technology regulation and offers policy recommendations for improving Kenya's digital credit landscape.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
B2C	Business-to-Consumer
CA	Communications Authority of Kenya.
CAK	Competition Authority of Kenya
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CBK	Central Bank of Kenya
CMA	Capital Markets Authority
COVID-19	Corona Virus Disease
DCP	Digital Credit Provider
DCS	Digital Credit Service
DFS	Digital Financial Services
DLAK	Digital Lenders Association of Kenya
DL	Digital Lender
DPA	Data Protection Act
DSP	Digital Service Provider
EC	European Council
EDPB	European Data Protection Board
EP	European Parliament
EU	European Union
FinTech	Financial Technology
FSD Kenya	Financial Sector Deepening Kenya
GIGO	Garbage In – Garbage Out
GDPR	General Data Protection Regulations
GPS	Global Positioning System
IA	Investigative Agency
ICCPR	International Covenant on Civil and Political Rights
IRA	Insurance Regulatory Authority
ITU	International Telecommunication Union
KLR	Kenya Law Reports
KRA	Kenya Revenue Authority
ML	Machine Learning
MNO	Mobile Network Operator
MSME	Micro, Small and Medium Enterprise

NBK	National Bank of Kenya
NSSF	National Social Security Fund
OECD	Organisation for Economic Co-operation and Development
ODPC	Office of the Data Protection Commissioner
PIN	Personal Identification Number
POPIA	Protection of Personal Information Act
SMS	Short Messaging Service
UN	United Nations
USA	United States of America
UDHR	Universal Declaration of Human Rights



LIST OF REGULATORY INSTRUMENTS

Constitution of Kenya, 2010.

Central Bank of Kenya (Digital Credit Providers) Regulations, 2022.

Data Protection Act, Chapter 411C.

Consumer Protection Act, No. 38 of 2016.

Central Bank of Kenya Act, Chapter 491.

LIST OF FOREIGN REGULATORY INSTRUMENTS

Regulation (EU) 2016/679 (General Data Protection Regulation)

Protection of Personal Information Act, 2013

LIST OF CASES

Coalition for Reform and Democracy (CORD) and 2 others v Republic of Kenya and 10 others [2015] eKLR.

Google Spain SL v Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González, Case C- 131/ 12, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317).

Kenya Legal and Ethical Network on HIV and AIDS (KELIN) and 3 others v Cabinet Secretary Ministry of Health and 4 others (2016) eKLR.

Węgrzynowski and Smolczewski v Poland, Appl. No. 33846/ 07, judgment of 16 July 2013.

Teresia Karungari v Branch Microfinance Bank, ODPC Complaint No. 0796 of 2023.

Musa Wesutsa v Azura Credit Limited T/A Truepesa, ODPC Complaint No. 1088 of 2024.

ACKNOWLEDGMENTS

I am grateful to my professor for his invaluable guidance, unwavering support and insights throughout this project. His expertise has been instrumental in shaping the direction and enhancing the quality of my research. I am eternally grateful to my parent Joseph Oundo PhD and Valerie Oundo for standing by me throughout this programme and for their constant support and guidance. I am grateful to my brothers and sisters-in-law Dr Emmanuel Oundo, Dr Benjamin Oundo, David Oundo Esq., Dr Maureen Oundo, Dr Mukami Ruoro-Oundo and Alice Oundo as well as my nieces and nephew; Nailah Oundo, Shannah Oundo, Mara Oundo and Nathan Oundo for being there for me and their constant support. I would also like to thank me for believing in me, I want to thank me for doing all this hard work, I want to thank me for having no days off, I want to thank me for never quitting, I want to thank me for just being me at all times. Most of all I want to thank God for everything, for without Him I would not have made it this far.

DEDICATION

This thesis is dedicated to my family, whose unwavering commitment and support to my education has profoundly affected my academic career and personal development, particularly my parents, Joseph Oundo PhD and Valerie Oundo. I am deeply thankful for their mentorship, constant motivation, and steadfast faith in me. Their guidance and support have been invaluable throughout this journey, shaping me into who I am today. This dissertation is a tribute to their endless sacrifices and profound impact on my life.

CHAPTER ONE

INTRODUCTION

1.1 Background

Banks have traditionally provided financial services through their branch networks. However, these are concentrated in cities or urban areas in developing countries.[1] To rectify this skewed availability of financial services, many governments have embraced Digital Financial Services (DFS) as an efficient means to increase financial inclusion.[2] DFSs can be defined as financial services provided through mobile phones and include e-money and mobile money delivered through bank-led and non-bank-led models.[3]

The digitalisation of the African financial sector has been deemed to have enormous potential to drive development and growth, although the accompanying risks must be appropriately managed.[4] With the rapid digitisation of the financial infrastructure, there has been greater financial inclusion, particularly with the 'unbanked' population. M-Pesa has increased the consumption and financial resilience of many Kenyan households, as was found by a 2016 study.[5] Furthermore, the study estimated that M-Pesa aided at least 200,000 households cross and live above the poverty line.[6] Micro, Small and Medium enterprises (MSMEs) have also been beneficiaries of the digital infrastructure due to the cheaper and more efficient financial services.[7] The Corona Virus Disease (COVID-19) pandemic further accelerated the uptake of digitised financial services not only in Kenya, but also globally.[8] Many policymakers pushed for digital payments to reduce the use of cash and to enable people and businesses to function despite the various restrictions on their movement.[9] By providing DFS through mobile money

---

1 Evan Gibson and Ross P Buckley, *Regulating Digital Financial Services Agents in Developing Countries to Promote Financial Inclusion* (SSRN Electronic Journal, 2015)

2 Evan Gibson *et al*, *Regulating Digital Financial Services Agents in Developing Countries to Promote Financial Inclusion'* (n 1).

3 Louise Malady and Ross P Buckely, *Building Consumer Demand for Digital Financial Services – The New Regulatory Frontier,* (CIFR Paper No 035/2014 (25 August 2014), 2.

4 Claudio Cali, Laura Wollny, Arthur Minsat and Elisa Saint Martin*, 'Digital Financial Services',* ' (European Investment Bank, 2021).

5 Tavneet Suri and William Jack, *The Long-Run Poverty and Gender Impacts of Mobile Money* (Sciencemag.org, Vol. 354, 6317, 2016).

6 ibid*,* (n 5).

7 Disse Sabrina and Sommer Christoph, *Digitalisation and Its Impact on SME Finance In Sub-Saharan Africa: Reviewing The Hype and Actual Developments,* (Discussion Paper No. 4/2020, Deutsches Institut für ntwicklungspolitik, Bonn). See also, Sahay Ratna., Ulric Eriksson von Allmen, Amina Lahrèche-Révil, A., Khera Purva, Ogawa Sumiko, Bazarbash Majid and Beaton Kim, *The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era*, (Departmental Paper No. 20/09, International Monetary Fund 2020).

8 ibid (n 4).

9 ibid (n 4).

and branchless banking services, providers can promote financial inclusion without physical access to a traditional bank branch.[10]

While many African banks have been expanding their digital services, digitalisation for DFSs has mainly been driven by new entrants into Africa's financial sector.[11] This move has significantly been bolstered by mobile money providers such as Safaricom and Airtel. For example, M-Pesa, created in 2007 by Vodafone and Safaricom, mainly in Kenya and Tanzania, triggered other Mobile Network Operators (MNOs) in Africa to adopt similar technology, such as MTN Mobile Money in West Africa.[12] Mobile money has played a critical role in developing DFSs in Africa by either complementing or supplementing existing financial providers.[13] The digitalisation growth trends in Africa remain on an upward trajectory.

1.1.1 Growth in Digital Financial Services in Kenya

The digitalisation of financial services in Kenya has seen significant growth and development. Some indicators of this include growth and development in mobile money services and commercial banks' substantial transition to digital channels for service delivery.[14] For instance, through branchless banking and the emergence of newer and often smaller non-bank Financial Technology (FinTech) companies to fill gaps of unserved demand for financial inclusion.[15] The number of FinTech companies and the range of services they provide has expanded rapidly since the launch of the mobile money provider M-Pesa.[16] Beyond financial services, the FinTech solutions being offered by several firms are seen as having the potential to revolutionise various sectors of the economy.[17]

Without undermining the importance of the growth as seen through the lenses highlighted above, of particular interest for this study is the significant growth in the realm of digital lending which has experienced significant growth that generally aligns with the developments in the DFS already highlighted, but not without its fair share of regulatory challenges. DCPs

---

[10] Kate Lauer, Denise Dias, and Michael Tarazi, *Bank Agents: Risk Management, Mitigation, and Supervision,* (CGAP Focus Note No 75, Washington, DC: CGAP, December 2011), 4 – 5 See also; Michael Tarazi, and Paul Breloff, *Regulating Bank Agents, CGAP Focus Note 68,* (Washington, DC: CGAP, March 2011).

[11] Cali Claudio *et al, 'Digital Financial Services',* 4.

[12] Disse Sabrina *et al., Digitalisation and its impact on SME finance in Sub-Saharan Africa: Reviewing the hype and actual developments,* (n 7). See also; GSMA, *State of the Industry Report on Mobile Money,* (2021a).

[13] Cali Claudio *et al, Digital Financial Services*, (n 4)

[14] ibid (n 1).

[15] Evan Gibson *et al*, *Regulating Digital Financial Services Agents in Developing Countries to Promote Financial Inclusion'* (n 1).

[16] Cali Claudio *et al, Digital Financial Services*, (n 4).

[17] ibid, (n 4).

are financial institutions that use technology to provide accessible loans in various amounts, durations and interest rates, and credit facilities via digital platforms. They use alternative data sources and innovative algorithms to quickly access creditworthiness, often resulting in near-instant loan approvals and disbursement. This allows them to accept a broader range of borrowers, including those without a formal credit history or collateral. Kenya has been at the forefront of providing digital lending solutions since the launch of M-Shwari in 2012. This led to the rapid proliferation of DCPs, with the number of licensed DCPs standing at fifty-eight (58) as of June 2024 and CBK recording receipt of five hundred and fifty (550) applications for licenses since March 2022.[18]

DCPs in Kenya often collect a wide array of consumer data for risk assessment, credit scoring and targeted marketing.[19] The types of data collected typically include personal identification information (PII) such as name and date of birth, financial transactions, device information such as the device model and SIM card details, and social media and behavioural data. The vast amounts of data collected raise concerns about how this information is managed, shared and potentially exploited. Financial Sector Deepening (FSD) Kenya, an independent trust dedicated to the achievement of a financial system that delivers value for a green and inclusive digital economy while improving financial health and capability for women and micro and small enterprises (MSEs),[20] has raised concerns regarding the practice of collecting sensitive information without clear explanations of its usage.[21] Furthermore, the data collected can also be monetised, used for targeted advertising or even sold to third parties without the consumer's consent. The Data Protection Act of 2019, which is lauded as being aligned with global standards, emphasises the principles of data minimisation, data security, right to access and informed consent. Despite these protections, enforcement remains a major challenge, as evidenced in the case of *Teresia Karungari v Branch Microfinance Bank.*[22] In this case the ODPC received a complaint from Teresia Karungari where she alleged that her right to privacy was breached by the respondent. The Complainant stated that the Respondent had been

[18] Central Bank of Kenya, Press Release, '*Licencing of Digital Credit Providers,'* (March 2024). https://www.centralbank.go.ke/uploads/press_releases/2069457347_Press%20Release%20-%20Licensing%20of%207%20Additional%20Digital%20Credit%20Service%20Providers.pdf

[19] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, (Journal of American Academy of Arts and Sciences, Daedalus, 2011) 38.

[20] Financial Sector Deepening, *About Us,* https://www.fsdkenya.org/about-us/who-we-are/ accessed on 27th March 2025.

[21] Francis Dwer, Jack Odero, and Edoardo Totolo, *'Digital Credit Audit Report: Evaluating the Conduct and Practice of Digital Lending in Kenya,'* (Financial Sector Deepening Kenya, September 2019) 1.

[22] ODPC Complaint No. 0796 of 2023.

spamming her email with messages claiming that she had not cleared her loan, yet she had cleared the loan in 2022. The Respondent admitted that it was due to an oversight that the Complainant was included in their list of default borrowers resulting in the unintended communication. The ODPC agreed that the Respondent erred in their actions.

1.1.2 Digital Credit Providers (DCPs) and Regulatory Challenges

Despite the benefits of digital lending services, their growth and development present significant challenges in the regulatory context in general and consumer data protection in particular. A few are worth highlighting to give context to the problem under research. The overarching challenge is that DCPs, also known as Digital Lenders (DLs), have taken advantage of the inadequacies in Kenya's regulation and proceeded to provide these services to the detriment of consumers.[23] Some of the manifestations of this challenge are highlighted below.

First is the manifestation associated with FinTech innovation and the broader space of new and emerging technologies. FinTech is the use of technological advances such as access to mobile phones, the internet, cloud computing and Artificial Intelligence (AI) to offer a wide range of financial services online or via mobile phones.[24] The development of DFSs, particularly digital credit, can lead to increased macro-financial risks, which, despite the existence of the DCP Regulations, are not adequately addressed by existing regulations.[25] Furthermore, the rise of FinTech brings with it new or heightened operational risks, including those related to cybersecurity and information technology failures.[26] Kenya has seen rapid growth in DFS, with high mobile phone penetration that has allowed Safaricom to reach over seventeen (17) million customers.[27] Coupled with advancements in technologies such as AI, which portends risks of misuse and problems of liability because of black box algorithm[28] – digital platforms often run algorithms and AI to enable recommendation engines, advice, pricing decisions and personalisation of customer experience which can be properly described as black box algorithms – problems, the

---

[23] Isaac Wachira Mwangi and Moses Sichei, *Determinants of Access to Credit by Individuals in Kenya: A Comparative Analysis of the Kenya National FinAccess Surveys of 2006 and 2009* (European Journal of Business and Management, Vol 3, No. 3) 217.

[24] Cali Claudio *et al, Digital Financial Services* (n 4).

[25] Cali Claudio *et al, Digital Financial Services* (n 4).

[26] Cali Claudio *et al, Digital Financial Services* (n 4).

[27] Timothy Lyman, Gautam Ivatury, and Stefan Staschen*, Use of Agents in Branchless Banking for the Poor: Rewards, Risks, and Regulation, CGAP Focus Note No 38*, (Washington, DC: CGAP, October 2006) 2.

[28] International Telecommunications Union, '*Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective,'* (ITU Telecommunication Development Bureau (BDT), Bill and Melinda Gates Foundation, 2016), 19.

challenge of consumer data breaches from this perspective remains complicated and generally unregulated in Kenya which gives rise to the contextual gap that this thesis seeks to address.

Exacerbating this challenge, and the second manifestation is the approach to FinTech innovation within the Central Bank of Kenya's (CBK's) regulatory ambit. While the Insurance Regulatory Authority (IRA) and Capital Markets Authority (CMA) have sandboxing environments for regulatory learning and responsible innovation support, the Central Bank of CBK) – which is the regulator of DCPs – seems not to have been interested in this approach to regulation. Having this as an issue is necessary because the extremely pervasive frontier technologies such as AI, blockchain and distributed ledgers, and big data analytics are heavily influencing business models that are being applied to DFSs, including digital credit services. This, perhaps, is a pointer to a weakness in the DCP regulatory framework, which is worsened by the pacing problem[29] that remains unaddressed by reactive approaches to regulation. This gives rise to a question as to whether informed consent is fit for purpose in these rapidly changing times.

The information asymmetries associated with the informed consent model, as the third manifestation, further aggravates the effects of the issues highlighted above.[30] According to Kemp, the traditional informed consent model has a weakness in effectively protecting the privacy of consumers' privacy. It inherently bears the risk of the 'informed' consumer agreeing to terms and conditions they fail to understand.[31] This is true of consumers in DCPs as consumers in DCP, in a bid to access funds at times in desperation, are likely to 'consent' to DCPs accessing their information without understanding how it is used and why it is required.[32] Furthermore, these agreements and policies may also state that they may be amended at any time without contacting the customer.[33] Besides, research has indicated that most consumers do not read privacy policies[34] mainly because it is time-consuming and that some consumers do not and cannot understand how their data is used, and shared and the resultant consequences.

---

[29] The Pacing problem is where technological innovation outpaces the ability of laws and regulations to keep up. Adam Thierer, *The Pacing Problem and the Future of Technology Regulation: Why Policymakers Must Adapt to a World That's Constantly Innovating,* (Mercatus Centre, George Mason University, Technology and Innovation August 8, 2018).

[30] Competition Authority of Kenya*, Report on the Competition Authority of Kenya Digital Credit Market Inquiry*, (2021), https://www.cak.go.ke/sites/default/files/Digital_Credit_Market_Inquiry_Report_2021.pdf

[31] Katherine Kemp and Ross P Buckley, *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (Georgetown Journal of International Affairs, Vol 18, No. 3, International Engagement on Cyber VII, 2017), 35-46.

[32] ibid (n 29).

[33] ibid (n 29).

[34] Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma* (Harvard Law Review 126), 1884-85.

Additionally, these terms are offered on a 'take it or leave it' basis which the consumer cannot bargain for their preferences.[35] This creates an information asymmetry that remains unresolved through regulation.[36] There are, however, other consent models that may present similar issues as those of the informed consent model, or otherwise present solutions that may address the issues. Implicit or implied consent is a contrast to the informed or explicit consent model. In this model, consent is inferred from the user's actions or behaviour rather than from a clear and affirmative statement. While this consent model can streamline user interactions by eliminating the need for multiple confirmation steps, it is less transparent than explicit consent. Therefore, implied consent is typically only used in low-risk scenarios, where the data being collected is not particularly sensitive.

Opt-in consent necessitates that users take explicit actions to express their agreement to the processing of their data, typically by actively checking a box or affirmatively responding to a request.[37] This approach guarantees that no presuppositions are made regarding consent and closely adheres to the principles of transparency and user sovereignty that form the foundation of data protection regulations. According to the GDPR, opt-in consent is generally mandated for most data collection practices, especially for actions such as direct marketing or the handling of sensitive information.

Granular consent enables individuals to consent to aspects of data processing instead of making a blanket acceptance or rejection of all data uses at once. This approach is especially beneficial in scenarios where various types of data are collected for different purposes.[38] Under the GDPR, granular consent is promoted to ensure that consent is specific, informed, and reflective of the individual's preferences. Nevertheless, implementing granular consent can be challenging for organisations, as it necessitates more advanced data management systems capable of monitoring and respecting individual consent choices across different types of data and purposes.

Dynamic consent represents a developing model that enables individuals to modify their consent choices as time progresses. This approach is particularly valuable in long-term data

[35] Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* (n 32) 1885. See also Gordon Hull, *Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data* (Ethics and Information Technology Journal, 17, 2015), 93-94.

[36] Patrick Eggimann and Aurelia Tamo, *Taming the Beast: Big Data and the Role of Law,* (Big Data and Privacy: Making Ends Meet, 28; Productivity Commission, "Data Availability and Use,") 67-68.

[37] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, (n 19) 34.

[38] Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* (n 32) 1885.

collection situations, such as medical research, where participants' privacy concerns and preferences may evolve during the study. Although it provides the greatest level of user independence and adaptability, it also poses challenges regarding implementation. Keeping consent records current with user preferences and ensuring that users are informed about changes in data processing activities can be demanding for most organisations.

Bundled consent refers to scenarios where consent for various data processing activities is combined, often compelling users to accept all terms or none. While this can simplify the consent process for organisations, it is frequently criticised for restricting user choice and control, as individuals might be obliged to agree to activities, they are uncomfortable with to access the service. The European Union (EU) General Data Protection Regulations (GDPR) established in 2016 dissuade bundled consent, especially when it concerns processing activities that aren't essential to the core functionality of the service delivered. Nevertheless, organisations are encouraged to present separate consent requests for distinct types of data processing, enabling users to make informed choices regarding each activity. This method corresponds with the principle of data minimisation, which aims to confine the collection of personal data to what is necessary for the intended purpose.

As a fourth manifestation, the data collected through the informed consent model, which finds its way into the big data ecosystem, may be used within the big data ecosystem in a manner that is eventually detrimental to the consumer and the wider digital credit market.[39] For instance, the use of automated borrower assessments is a predatory strategy commonly employed by digital lenders, often without the informed consent of the borrower.[40] This includes utilising call logs, global positioning system (GPS) data, social network information, and contact lists that have been used to threaten consumers or their associates in the past.[41] Some researchers have established that this leads to intrusion into a creditor's privacy by establishing evidence-based patterns arrived at through the use of algorithms often associated with AI.[42] Such patterns include the most likely time for responsiveness to communications,

[39] Arjuna Costa, Anamitra Deb, and Michael Kubzansky, *Big Data, Small Credit: The Digital Revolution and Its Impact on Emerging Market Consumers* (Innovations, 10, 2015), 49-80.

[40] Jonathan Greenacre, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (Washington University Journal of Law and Policy, Vol. 61, 2020), 229.

[41] Katherine Kemp *et al*, *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,*(n 29) 35-46.

[42] Christophe Hurlin, Christophe Pérignon, *Machine Learning Et Nouvelles Sources De Donnes Pour Le Scoring De Crédit*, (Revue d'économie financière, Technologies et Mutations de l'Activité Financière, 2019) 21.

travel history, location history, and gambling history.[43] Since algorithms could have biased parameters or utilise biased data, are applied in arriving at target measures such as unsolicited marketing using the utilisation of big data to identify patterns within a predicted set.[44] Corollary questions, such as those to do with personalised distortive or discriminatory pricing guided by algorithms– are a real problem to the DCP market and competition.[45] Unfortunately, the use of this data can lead to the exclusion of the very vulnerable group that these tactics were intended to assist in the first place.[46] This poses serious questions about the effectiveness of the CBK (Digital Credit Providers) Regulations, 2022 (DCP Regulations), as well as the data privacy and protection regimes applicable in such circumstances.

Consumer data protection, as evidenced above, is essential to the preservation of individual privacy, maintaining trust in digital systems, and ensuring compliance with regulatory requirements and standards. While legal frameworks such as the GDPR, DCP Regulations and the Data Protection Act are crucial, the ethical importance of protecting consumer data is equally important. Consumer privacy can be considered a human right. Article 31 of the Constitution of Kenya declares that no one shall be subject to arbitrary interferences to their privacy. This is because, on one hand, businesses derive substantial value from the use of personal data to enhance services and improve customer targeting and on the other hand, poor data protection practices can result in substantial economic pressure to the company due to fines, suits and reputational damage; and personal losses to the consumers due to the protracted legal suits.

The fifth manifestation is associated with personalised as well as differential possible discriminatory pricing. The interest and loan fees payable in digital credit transactions are typically higher compared to[47] Kenyan commercial banks' average interbank lending rate as of March 2024 was reported to be approximately 13.42% per annum.[48] For instance, Tala charges[49] interest rates of between 7% and 17% on any facilities issued to customers for 30

[43] Katherine Kemp *et al*., *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (n 23) 35-46.

[44] Jonathan Greenacre, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (n 38) 229.

[45] Gerhard Wagner and Horst Eidenmüller, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,* (The University of Chicago Law Review, 2024).

[46] Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,* (n 43).

[47] Jonathan Greenacre, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (n 38) 229.

[48] Central Bank of Kenya, '*Interest Rates Statistics,'* 'Interest Rates | CBK' (March 2024) <https://www.centralbank.go.ke/statistics/interest-rates/> accessed 1 March 2024.

[49] Tala Kenya, 'Tala Loans Kenya | Download the Tala Loan App (10M+ Installs)' (March 2024) <https://tala.co.ke/tala-app-download-google-play-store-kenya/> accessed 1 March 2024.

days.[50] OKash, on its part, charges an interest rate of up to 36% per annum.[51] Branch,[52] another popular digital lender in Kenya charges interest rates of between 10% and 27%[53] based on the facility amount and the repayment history of the borrower.[54] Some digital lenders have argued that what they charge is not interest but rather costs or administrative fees for the risk.[55] These generally align with findings of a 2021 inquiry conducted by the Competition Authority of Kenya (CAK), which established that the penalty fees incurred by borrowers have a median and mean cost of 12% and 52%, respectively.[56] The DCP Regulations only provide for interest on non-performing loans and fail to extend a base lending rate as it does for commercial banks, which is a major weakness of the regulations. Through FinTech innovations, DCPs collect big data and use sophisticated AI to learn from and execute tasks based on the data with the possible result in varying interest rates on consumers, which may differ between them.[57] The informed consumer model further aggravates this issue in that many consumers may not understand that such data is being collected and how it is used to affect the interest rates on their loans, which may result in a high number of non-performing loans.[58]

Another challenge, and a sixth manifestation, pertains to consumer choice within the DFSs ecosystem, particularly in Kenya. This challenge stems from the heavy reliance on payment systems, notably M-Pesa, within the ecosystem. M-Pesa dominates the mobile money market with a staggering 97.1% market share, according to the Communications Authority of Kenya's (CA's) Sector Statistics for the Second Quarter Financial Year 2024. The increasing dominance of M-PESA-affiliated lenders in digital lending also raises concerns about consumer choice and competition, potentially impacting consumers negatively.[59] The impact could be extensive

---

[50] Jonathan Greenacre, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (n 38) 229.

[51] Jackline Wangari, *OKash, Loan Application Requirements, Interest Rates, Terms and Conditions - Tuko.Co.Ke'* (Tuko.co.ke, March 30, 2021.) <https://www.tuko.co.ke/288602-okash-loan-application-requirements-interest-rates.html> accessed 1 March 2024.

[52] Jonathan Greenacre, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (n 38) 229.

[53] Branch Kenya, 'Branch Kenya | FAQs' (March 2021) -<https://branch.co.ke/faq>- accessed 1 March 2024.

[54] 'Branch Kenya | FAQs' -, https://branch.co.ke/faq- accessed 1 March 2024 (n31).

[55] Jonathan Greenacre, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (n 38) 229.

[56] Competition Authority of Kenya*, Report on the Competition Authority of Kenya Digital Credit Market Inquiry*, (2021).

[57] International Telecommunications Union, *Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective,* (n 26) 43.

[58] ibid (n 26) 44.

[59] Lech Gąsiorkiewicz and Jan Monkiewicz, *Digital Finance and the Future of the Global Financial System Disruption and Innovation in Financial Services*, (Routledge, 1st Edition, New York), 213. Factbox: *EU Rules Aim to Increase Choice in Customer Payments.* Factbox: EU rules aim to increase choice in customer payments | Reuters

in the space of consumer data as network effects and the concentration of data around a few players in the DCS market further complicate this.

These manifestations have generally been seen through predatory/discriminatory interest rates, personal data abuses and unethical debt collection practices perpetrated by DCPs.[60] As a result of these, Kenya purged all digital lending companies without licences in 2022. To address these excesses, the CBK (Digital Credit Providers) Regulations, 2022 (referred to as the DCP Regulations) were enacted into law. These regulations introduced data protection provisions to protect borrowers by bringing DCPs under the ambit of regulation.[61] These regulations complement and largely echo the data protection provisions in the Data Protection Act of 2019 and the Consumer Protection Act of 2012, which had been in place when the symptoms of the problem highlighted above were manifesting.

1.2 Statement of the Problem

This research investigates the adequacy of the informed consent model as applied within Kenya's legal and regulatory framework for consumer data protection in digital credit services. Despite the introduction of legislation such as the DCP Regulations of 2022, the Data Protection Act of 2019 and the Consumer Protection Act of 2012, significant threats to consumer data privacy persist, indicating the glaring gaps within the frameworks themselves and their implementation.

These gaps are evidenced in several instances such as the rapid and unchecked innovation of FinTech, insufficient regulatory adaption by the CBK, and information asymmetries inherent in the informed consent model. Furthermore, the challenges within the big data and AI ecosystem, anti-competitive risks linked to consumer choice, and predatory conduct by DCPs further exacerbate these challenges. However, the core of the problem lies in the inadequacy of and ineffectiveness of the informed consent model to address these challenges. The research gap this thesis seeks to fill is the contextual gap in this type of research.

1.3 Objectives of the Research

The general objective of this study is to critically examine the efficacy of the legal and regulatory frameworks governing consumer data protection in digital financial services with

---

[60] Jactone Lawi, '*CBK Blames Legal Void for Inaction on "rogue" Digital Lenders'* (The Star, December 2023) <https://www.the-star.co.ke/business/kenya/2023-12-05-cbk-blames-legal-void-for-inaction-on-rogue-digital-lenders/> accessed 8 July 2024.

[61] Mutete Cynthia, Indokhomi Dominic, *Kenya: Regulation of Digital Lenders in Kenya | Bowmans* (April 2022) <https://bowmanslaw.com/insights/kenya-regulation-of-digital-lenders-in-kenya/> accessed 8 July 2024.

specific reference to consumers of digital credit services. In pursuit of this general objective, the specific objectives of the study are to:

(a) Evaluate the different types of consent models within the context of the rationale, development, scope, and challenges related to consumer data protection in digital credit services in Kenya.

(b) Critically analyse the adequacy of the informed consent model within the legal and regulatory frameworks governing consumer data protection in digital credit services.

(c) Assess legislative and regulatory practices in the European Union (EU), and South Africa to draw lessons on useful practical approaches and experiences for consideration in improving Kenya's legal and regulatory regime applicable to consumer data protection of digital credit services.

1.4 Research Questions

As its overarching research question, this thesis questions the efficacy of the legal and regulatory frameworks applicable to the protection of consumers of digital credit services in Kenya. This overriding question raises the following specific questions:

(a) What are the different types of consent models within the rationale, development, and scope of consumer data protection in digital credit services in Kenya?

(b) Is the informed consent model within the legal and regulatory framework governing consumer data protection sufficient to address the issue of consumer data collection and use in digital credit services in Kenya?

(c) What lessons on useful, practical approaches and experiences can Kenya learn from the EU, and South Africa to enable it to improve Kenya's legal and regulatory regime applicable to consumer data protection of digital credit services?

1.5 Justification of the Research

While there are studies that have been done on the DFSs sector, particularly in digital lending, there is a dearth of data in Kenya concerning consumer data protection within the DCSs. This study attempts to add to the existing body of literature while also attempting to reduce the literature gap within the field of study. The DCP Regulations attempt to remedy the gap in legislation; however, its provisions are still insufficient in addressing consumer and data protection. In doing so, the researcher hopes that the study's findings and recommendations will be beneficial to several stakeholders impacted by the problem, such as policymakers, lawmakers, researchers, consumers, and academics in the field of financial law.

The policymakers will benefit from this study in that it will inform how policies should be further shaped and applied concerning the handling and protection of consumers and their data. The body of research allows them to understand the pitfalls within the current policies and allow them to amend them to fit the Kenyan context. Similarly, lawmakers would benefit from this thesis in that the current legislation is still insufficient in overseeing the growing landscape of data protection, particularly with the growing use of AI. This study aids them in understanding the development and use of big data and AI so that they will not be victims of the pacing problem. Furthermore, researchers would benefit in that there would be a compilation of current literature and an indication of potential areas of study. It would also allow them to have an in-depth body of research that they can reference while seeking out potential areas of study and providing answers to questions within the current academic landscape. Similarly, academics would benefit in that it attempts to address potential knowledge gaps within Kenyan financial law and regulation. Consumers would also benefit from understanding how their rights are either protected, violated, or ignored because of the implementation of various policies, laws, and regulations. They would also understand the different types of consent models, how they are affected, and how to better evaluate their rights, duties and responsibilities within the rapidly changing digital credit landscape.

1.6 Hypothesis

The organising hypothesis of this study is that the legal and regulatory frameworks applicable to the protection of consumers of digital credit services, including in Kenya, have a fundamental bearing on the full realisation of those rights. This organising hypothesis is premised on the fact that the legal and regulatory frameworks governing the informed consent model in digital credit services in Kenya are inadequate, and fundamental questions arise about whether they are optimally fit for purpose.

1.7 Theoretical Framework

The researcher was be guided by a blend of private and public interest theories of regulation; the technology acceptance model (TAM) theory as well as the information asymmetry theory in pursuing a feasible solution to the questions raised in this research.

1.7.1 Public and Private Interest Theory

To start with, the private interest theory, also known as the economic theory of regulation, posits that regulatory policies are often designed to serve the interests of private individuals or

groups, often to the detriment of the public good. [62]This theory suggests that regulatory agencies can be influenced or "captured" by the industries they are supposed to regulate, leading to regulations that benefit industry participants by reducing competition and increasing market power. [63]

There are various points of note within the private interest theory. First, its private interest potential to advance regulatory capture.[64] According to Stigler, regulatory capture occurs when the interests of the industries dominate the regulatory agencies, they oversee rather than the public they are meant to protect. [65] It is the argument of the proposed research that the general inadequacy surrounding the informed consent model in consumer data protection is symptomatic of general regulatory inaction – a broader manifestation of regulatory capture. The second aspect of the private interest theory is its characterisation of rent-seeking behaviour wherein private entities invest resources in lobbying to secure economic rents from regulation.[66] This behaviour, as Tullock highlights, results in regulations prioritising a few peoples' or groups' financial interests over the broader public interest.[67] Again, it is the argument of the proposed research that the general inadequacy surrounding the informed consent model in consumer data protection in DCS is symptomatic of possible successes of DCPs in securing economic rents, even if this may be temporal. Peltsman provides a perspective on the rent-seeking aspect of private interest theory when he provides empirical analyses showing that regulated industries often end up with policies that enhance their profitability at the expense of consumer welfare.[68] The DCSs are highly profitable due to their higher interest rates as well as the costs of compliance with data protection regimes generally offset by loopholes in compliance. This fails to consider that the consumers' (digital) literacy levels impede their understanding of the terms they are being subjected to, the kind of data being collected, how the data is to be used, and the resultant asymmetries of information.

In contrast to the private interest theory, public interest theory views regulation as a tool to correct market failures and promote the overall welfare of the public. It assumes that regulators

---

62 Ernesto Dal Bo., *Regulatory Capture: A Review*, (Oxford Review of Economic Policy, 22, 2, 2006), 203-225.
63 ibid (n 60) 203-225.
64 ibid (n 60) 203-225.
65 George Stigler, G.J., *The Theory of Economic Regulation*, (The Bell Journal of Economics and Management Science, Vol. 2, No. 1, 1971), 3-21.
66 Gordon Tullock, *The Welfare Costs of Tariffs, Monopolies, and Theft*, (Western Economic Journal, Vol. 5, No. 3, 1967), 224-232.
67 ibid (n 64) 224-232.
68 Sam Peltzman, *Toward a More General Theory of Regulation*, (Conference on the Economics of Politics and Regulation, Vol. 19, No. 2, 1976), 211-240.

act in the public's best interest to address issues such as monopolies, externalities, and information asymmetries.[69] According to Pigou, the main proposition of the public interest theory is the correction of market failure where government intervention is necessary to correct market inefficiencies that arise from externalities and other forms of market failure, including failures occasioned by the negative effects of private interest propositions in the private interest theory.[70] Posner emphasises the importance of regulation in ensuring, among others, equitable access and fairness in the market, protecting consumers from exploitation, and promoting social welfare.[71] This theory underscores the role of regulation in safeguarding public goods and services, which are typically underprovided in unregulated or underregulated markets. The digital credit market was, for a long time, an unregulated market and even now, with the DCP Regulations in place, among other laws applicable to consumer data protection, it remains underregulated in certain aspects, especially with respect to the models of data protection applied in the prevailing legislation.

Overall, the private interest theory generally underscored the researcher's perspective on how private actors generally tend to steer regulation and policy towards their private interests more than consumer interests. The private interest theory shaped the researcher's interrogation of the interface between the law and the DCPs' actions concerning the consumers. The public interest theory further informs the relationship between the government, the DCPs and the consumers. The researcher's reliance on these theories is based on their classical argument of whether to allow private actors to inform the law or whether public interest should supersede private interest and whether there can be a balance. By analysing the historical context, regulatory bodies, the influence of interest groups, and regulatory outcomes, the study aims to provide a comprehensive understanding of the interplay between private interests and public welfare in the regulation of DFSs.[72]

1.7.2 Information Asymmetry Theory

Information asymmetry refers to an instance where one party in a transaction or interaction, in this case, the DCPs, possess more or better information than the other party, the consumer. This imbalance of information can lead to market inefficiencies, distorted or mistaken decision-

[69] Robert Baldwin, Martin Cave, and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, (Oxford University Press, Oxford, 2nd Edition, 2012).

[70] Arthur Cecil Pigou, *The Economics of Welfare*, (London: Macmillan and Co, 4th Edition, 1932).

[71] Richard Posner, *Theories of Economic Regulation*, (The Bell Journal of Economics and Management Science, RAND Corporation, Vol. 5, No. 2, 1974), 335 -358.

[72] Roger Noll, *Economic Perspectives on the Politics of Regulation*, (Handbook of Industrial Organisation, Vol, 2, 1989) 1253-1287.

making and have the potential for market failure. This theory can be applied in many instances, such as economics, finance, insurance, labour markets and other domains. In this theory, it is important to understand some of its important aspects: adverse selection, moral hazard, and the roles of signalling and screening in transactions. In this section, this study delves into a brief explanation of the origins of the theory, the major contributors of the theory, and its implications on the consumers and the DCPs.

Information asymmetry theory gained prominence in the 1970s through the pioneering work of George Akerlof, Michael Spence, and Joseph Stiglitz. These economists aided in formalising the understanding of how unequal information distribution between parties in markets can affect decision-making and market outcomes.

George A. Akerlof's 1970 paper, the Market for Lemons, is one of the earliest and most influential works on information asymmetry.[73] In his paper, Akerlof examined the used car market to demonstrate how sellers generally have more information about the quality of their cars than buyers.[74] He argued that this information gap could lead to adverse selection, where low-quality goods crowd out high-quality goods from the market.[75] Applying the same example to the context of this study, the DCPs have more information about the amount of money they can lend out, how their systems work in rating potential consumers, their loan liabilities, and their creditworthiness. This information gap could lead to instances whereby the DCPs grant higher rates to potential defaulters as compared to those who repay faster. This would flood the market with cheaper loans, thus threatening the formal banking system. Furthermore, the consumers would be unsure whether their repayment rate is higher or lower than other consumers and thus would be forced to repay at the stated rate without knowing what the average rate is or would be. Akerlof's work highlighted the potentially devastating consequences of information asymmetry in markets, including market failure, market inefficiencies and consumer mistrust. His insights have been applied to various industries not limited to but including finance, insurance and labour markets.

In 1973, Michael Spence introduced the concept of *signalling* to address information asymmetry.[76] Signalling occurs where the more informed party (the DCPs) in a transaction sends signals to the less informed party (the consumers) to convey information about their

[73] George Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism,* (The Quarterly Journal of Economics, Vol. 84, No. 3, 1970) 488 – 500.
[74] ibid (n 71) 488 – 500.
[75] ibid (n 71) 488 – 500.
[76] Michael Spence, *Job Market Signaling,* (The Quarterly Journal of Economics, Vol. 87, No. 3, 1973), 355 – 374.

ability, quality or intentions. Spence's primary example of signalling was in the job market, where employers are uncertain about the abilities of potential employees.[77] A job candidate can "signal" their competence by acquiring a degree or professional certification, which serves as a proxy for their skill level. Although the degree itself may not directly enhance productivity, it serves as a credible signal to the employer about the candidate's quality. Spence's signalling model has since been applied beyond the labour market to corporate finance, for example, where firms might signal their financial strength by paying dividends or investing in costly advertisements to demonstrate their market leadership. This would be the same case where DCPs advertise themselves as giving the cheapest loans, utilising the lowest rates, however, they may be utilising big data to determine the range by which they need to charge you based on your borrowing history or any other information.

Joseph Stiglits further developed the theory by focusing on *screening.*[78] This is a method used by the less informed party to elicit information from the more informed party. Stiglits's research, particularly on insurance markets, explored how companies can design policies that incentivise individuals to reveal their true risk profiles.[79] For instance, in health and vehicle insurance, insurers often offer a range of plans with varying deductibles and premiums.[80] Individuals who know they are low risk are more likely to choose policies with high deductibles with low premiums, while high-risk individuals might opt for lower deductibles and higher premiums. This process of self-selection enables insurers to screen applicants effectively and reduce the information gap. In the present context, this might present itself through the terms and conditions offered by the different DCPs act like the premiums offered by the insurance companies. They then use these terms and conditions to impose upon the consumer a range of rates that they offer depending on their creditworthiness. The consumer may fall under one of the rates following an investigation into their creditworthiness and the DCPs assuming that the consumer is adequately informed would lead to automated decision-making which would then become a pitfall in the informed consent model.

Together, Akerlof, Spence and Stiglits laid the foundation for a comprehensive understanding of information asymmetry, its impact on markets and potential solutions to mitigate its effects.

---

[77] ibid (n 74) 355 – 374.
[78] Joseph Stiglitz, *The Theory of "Screening," Education, and the Distribution of Income,* (The American Economic Review, Vol. 65, No. 3, 1975) 283 – 300.
[79] ibid (n 76) 283 – 300.
[80] ibid (n 76) 283 – 300.

1.7.3 Technology Acceptance Model Theory

The TAM was developed as an extension of Ajzen and Fishbein's Theory of Reasoned Action (TRA),[81] a general theory of behaviour that posits that an individual's intention to engage in a particular behaviour is determined by their attitude toward the behaviour and subjective norms.[82] Davis adapted this framework to the context of technology use, focusing on how users form intentions to adopt and use information systems.

In his original 1989 study, Davis proposed two core constructs – perceived usefulness (PU) and perceived ease of use (PEOU) – which are the primary determinants of user acceptance of technology.[83] These two constructs were shown to have a significant impact on an individual's attitude towards using the technology, which in turn influenced their behavioural intention to use it.[84] The model assumes that if users perceive a technology as useful and easy to use, they are more likely to have a positive attitude toward it and consequentially be more willing to use it. This explains the prominence of mobile banking and the rapid proliferation of digital credit apps in Kenya.

The TAM has provided a robust framework for understanding how and why individuals accept and use new technologies. Its core constructs offer valuable insights into the factors influencing technology adoption across various industries and contexts. TAM has also been extended and adapted over time, resulting in more compressive models like TAM 2,[85] TAM 3 and Unified Theory of Acceptance and Use of Technology (UTAUT),[86] as discussed, which account for additional factors such as social influence, user experience, and individual preferences.

1.8 Literature Review

There has been minimal study in Kenya related to digital lenders. However, this section attempts to delve into relevant literature in the study area. Several authors have attempted to conduct an in-depth study of the various legal provisions in Kenya that may affect consumer protection and digital lending. However, the available literature is limited to the extent that it is not specifically dedicated to consumer data protection through in-depth analyses of specific

[81] Fred Davis, *Perceived Usefulness, Perceived Ease Of Use, And User Acceptance Of Information Technology,* (MIS Quarterly, 13(3), 1989), 319 – 340.
[82] ibid (n 79), 319 – 340.
[83] ibid (n 79), 319 – 340.
[84] ibid (n 79), 319 – 340.
[85] Viswanath Venkatesh, and Fred Davis, *A theoretical extension of the technology acceptance model: Four longitudinal field studies*, (Management Science, Vol. 46, No. 2, 2000), 186 – 204.
[86] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D Davis, *User acceptance of information technology: Toward a unified view*, (MIS Quarterly, Vol. 27, No. 3, 2003), 425 – 478.

differences in various laws and their legal implications in Kenya. More particularly, the literature is not focused on analysing the adequacy of the informed consent model and its alternatives in the protection of consumer data in Kenya. Moreover, the literature specific to informed consent models in consumer data protection in DCSs generally concerns other jurisdictions, thus leaving a gap in Kenya. On this account, the literature was reviewed in two clusters: data protection and consumer protection. In the former cluster, the literature reviewed mainly speaks to what kind of data is collected and the various general investigations into the Kenyan financial sector. However, the literature reviewed under this cluster is scarce on the protection and enforcement mechanisms of consumer data protection in DCSs in Kenya. On its part, the literature reviewed under the latter cluster.

1.8.1 Data Protection and Big Data

Financial Sector Deepening (FSD) Kenya[87] conducted an audit of the digital credit facilities in Kenya, where the digital credit facilities in Kenya are coming under increased scrutiny for their lack of regulation and potential privacy issues. FSD Kenya further notes that financial institutions have raised concerns about the potential for fraudulent loan applications and the lack of oversight regarding data collection and storage.[88] According to FSD Kenya, these institutions argue that while the low barriers to entry promote efficiency, they also make it easy for malicious entities to enter the market and engage in extensive data mining with minimal oversight.[89] The study also highlights the types of data collected by lending apps, including sensitive information such as economic status, Kenya Revenue Authority (KRA) Personal Identification Number (PIN), contact details, and access to personal communication and location data.[90] Additionally, the report raises concerns about the lack of clarity regarding how consumer data is used and shared, as well as the potential implications of big data analytics and AI in the collection of this data. While it identifies aspects of the problem under this research, FSD Kenya fails to address the various consent models that impact the handling of consumer data in DCSs, as well as how big data analytics and AI are leveraged in the collection and use of this data. This creates a knowledge gap, which this study intends to address.

---

87 Francis Dwer, Jack Odero, and Edoardo Totolo, *Digital Credit Audit Report: Evaluating the Conduct and Practice of Digital Lending in Kenya,* (Financial Sector Deepening Kenya, September 2019) 1.

88 ibid (n 85) 11-13.

89 ibid , (n 85) 13.

90 ibid , (n 85) 11.

Kemp and Buckley[91] observe that big data analytics and other data-driven innovations have been adopted within the financial services sector particularly within developing countries, to offer credit to consumers without a formal credit history. Kemp and Buckley adds to the discussion that the 'informed consent' model that has been adopted and is still utilised, has a weakness in effectively protecting consumer privacy despite offering accessible credit facilities.[92] Kemp and Buckley state that the informed consent model assumes that the consumers fail to understand what they are agreeing to.[93] They also state that consumer consent cannot be the central solution to the data protection problem for financial services in developing countries such as Kenya.[94] The gap that persists in this paper is with respect to alternatives to the informed consent model and consumer consent exist that may remedy the current situation. Besides, these risks were observed in a context that is not Kenya's and in 2017 before Kenya enacted the DCP Regulations and the Data Protection Act, hence a contextual gap that this study seeks to reduce.

Wagner and Eidenmüller[95] contend that the emergence of big data and AI is leading to new Business-to-Consumer (B2C) interactions as companies accumulate extensive sets of information about consumer preferences, behaviour, and assets. According to Wagner and Eidenmüller, much of the existing literature on the impact of these advanced technologies on B2C transactions assumes a beneficial use of the gathered data.[96] They also claim that companies are exploiting common consumer biases in a deliberate manner.[97] They further elaborate that these companies have effectively utilised the distinctive biases and may be able to manipulate individual biases with the assistance of big data analytics and AI.[98] They conclude that the belief that big data analytics can enhance consumer contentment and

---

91 Katherine Kemp *et al*., *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (n 23) 35-46.

92 Katherine Kemp *et al*., *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (n 23) 35-46.

93 Katherine Kemp *et al*., *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (n 23) 35-46.

94 Katherine Kemp *et al*., *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (n 23) 35-46.

95 Gerrard Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences'* (n 43), 592.

96 Gerrard Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences'* (n 43), 592.

97 Gerrard Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,'* (n 43), 592.

98 Gerrard Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,'* (n 43), 594.

allegiance has been challenged, as it seems to be the opposite.[99] In a position shared with Kemp and Buckley, Wagner and Eidenmüller further elaborate that many consumers fail to read and understand the fine print in the terms and conditions presented to them in transactions, and the legal requirements for businesses to flag issues in such forms are not of much use to less tech-savvy consumers.[100] Wagner and Eidenmüller's work was a review conducted in the USA and EU, which are different jurisdictions with different practices from Kenya, thus presenting a contextual gap within the literature. This study attempts to remedy this contextual gap by trying to understand whether both jurisdictions suffer from similar issues, whether there are more unique issues in Kenya, and what potential regulatory and policy responses may be applied in one or both contexts.

Eliaz and Spiegler[101] support Wagner and Eidenmuller's assertion when they argue that big data and AI also offer incentives to take advantage of naïve or biased customers. Competitive pressures may force businesses to engage in exploitative practices.[102] Eliaz and Spiegler's study, however, fails to underscore how policy and legislation should be shaped, particularly with reference to the Global South and their resultant effects on consumer data protection, hence a gap that this research seeks to reduce.

Mothibi and Lazaridis,[103] researching under the ambit of the Financial Sector Conduct Authority (FSCA) of South Africa, investigated FinTech digital platform activity in South Africa and their regulatory implications where they identified various areas of consideration, including digital platforms requiring liability and ethics framework governing their data and consumer protection measures alongside registration. Mothibi and Lazaridis note that there is a growth in the prominence of digital platform-based businesses and describes a digital platform as a technology-enabled business model that creates value by facilitating exchanges

---

99 Gerrard Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,'* (n 43), 595.

100 Gerrard Wagner *et al.*, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,'* (n 43), 596.

101 Kfir Eliaz and Ran Spiegler, *Contracting with Diversely Naive Agents*, (The Review of Econmic Studies, Vol. 73, Issue 3, July 2006), 689 – 690.

102 Michael Grubb, *Overconfident Consumers in the Marketplace*, (Journal of Economic Perspectives, Vol. 29, Issue 4, November 2015) 9,12–13. See also; Xavier Gabaix and David Laibson, *Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets*, (Quarterly Journal of Economics, Vol. 121, May 2006) 505, 507–11. See also; Stefano DellaVigna and Ulrike Malmendier, *Contract Design and Self-Control: Theory and Evidence*, (Quarterly Journal of Economics, Vol. 119, 2004) 353,389.

103 Kagiso Mothibi and Dino Lazaridis, *Fintech Digital Platforms – An Investigation into Fintech Digital Platform Activity in South Africa and Their Regulatory Implications: Research Document,* (Financial Sector Conduct Authority, 2021) 3.

(the intermediation of services) between consumers and financial product producers.[104] There are various types of digital platforms, such as technology platforms, computing platforms, utility platforms, interaction platforms, marketplaces, on-demand platforms, crowdsourcing platforms and data harvesting platforms[105] (with which this study is concerned). Mothibi and Lasaridis identify risks associated with digital platforms, such as anti-competitive practices, data breaches, lapses in regulation across borders and lack of consumer education. The report presupposes a research gap regarding black-box algorithms, data breaches and consumer protection within the context of South Africa, leaving a contextual gap that this study intends to reduce.

Hurlin[106] defines Machine Learning (ML) as a big data technique employed for collecting, analysing, and utilising consumer data. He notes that ML involves the use of algorithms to address issues and enhance performance through learning from experience, without human involvement.[107] Hurlin asserts that ML empowers algorithms to generate new predictions by combining and altering the original predictors. [108] Additionally, Hurlin points out that ML can be applied in assessing credit risk, where new data is used to evaluate a borrower's creditworthiness.[109] The paper further examines the increasing significance of ML in risk scoring and presents its insights from both a French and a data science perspective, revealing a gap in context and discipline. On its part, the study proposed herein attempts to strike a balance between the data science perspective and the legal perspective, while also attempting to understand what lessons Kenya can draw from foreign jurisdictions and whether consumer data can be protected or are there any other alternatives available.

While agreeing with Hurlin, Medine[110] asserts that the borrower's information could be utilised to assess an individual's creditworthiness and for other purposes as determined by the DCP, such as targeted advertising. Medine also contends that the use of relatively new and unproven algorithms could result in inaccurate and harmful evaluations of an individual's creditworthiness.[111] Medine's research leaves a gap in the study of the legal implications of the

[104] Kagiso Mothibi *et al.*, *Fintech Digital Platforms – An Investigation into Fintech Digital Platform Activity in South Africa and Their Regulatory Implications: Research Document,* (n 101) 4.
[105] Kagiso Mothibi *et al.*, *Fintech Digital Platforms – An Investigation into Fintech Digital Platform Activity in South Africa and Their Regulatory Implications: Research Document,* (n 101) 5.
[106] ibid (n 40) 21.
[107] ibid (n 40) 23.
[108] ibid (n 40) 23.
[109] ibid (n 40) 23.
[110] David Medine, *Making the Case for Privacy for the Poor,* (CGAP Blog, November 15, 2016) 1.
[111] ibid (n 108) 1.

use of untested and unchecked ML algorithms and AI within various contexts, especially in Kenya, which is currently experiencing a sudden surge in the uptake of AI and ML. Besides, the study does not have Kenya as its jurisdiction of focus hence a contextual gap that the proposed study seeks to reduce.

Lokke and Corein[112] argue that certain data sets may exhibit bias against individuals based on race and gender, despite constitutional provisions prohibiting discrimination on such grounds. This represents a significant drawback in machine learning, as highlighted in Lokke and Corein's work.[113] The utilisation of such a biased system in conjunction with credit scoring and extensive consumer data sets could result in further adverse conditions for borrowers.[114] The study leaves a gap in context and legal criticism of data protection laws available that regulate AI and ML, particularly in DCSs.

Pazarbasioglu *et al*'s[115] analysis indicates that DFSs have played a pivotal role in enhancing access to financial products and services for individuals and businesses in both developing and developed nations. However, they argue that there are certain drawbacks associated with the widespread adoption of DFS, particularly relating to consumer protection.[116] Pazarbasioglu *et al* observe that one of the major challenges is the prevalence of fraudulent activities within the digital financial space. While consumer protection regulations have been implemented to address these concerns and mitigate information disparities between consumers and DCPs, it is important to note that these measures may not entirely eradicate the existing information imbalances. These authors indicate the prevalence of machine learning in digital scoring has severe impacts on consumer data protection mechanisms. These impacts have yet to be elaborated upon with clear reference to DCPs which this study intends to clarify.

1.8.2 Consumer Protection

Yaworsky *et al*[117] note that the data handling practices of the DCPs could potentially expose consumers to a higher risk of receiving inappropriate marketing for products and services, as this data might be utilised to promote more products and services to boost profits. This suggests

---

[112] Lokke Moerel and Corien Prins, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things,* (Tilburg Law School, May 25, 2016), 22.

[113] ibid (110) 22.

[114] ibid (110) 22.

[115] Ceyla Pazarbasioglu, Alfonso Garcia Mora, Mahesh Uttamchandani, Harish Natarajan, Erik Feyen and Mathew Saal, *Digital Financial Services*, (World Bank Symposium, 2020)*,* 54.

[116] ibid (n 113) 54.

[117] Katherine Yaworsky, Dwijo Goswami, and Prateek Shrivastava, *Unlocking the Promise of (Big) Data to Promote Financial Inclusion,* (Accion Global Advisory Solutions, Accion Insights, March 2017) *9-11, 29-33.*

that consumer protection measures do not provide absolute security.[118] It also highlights the existing gap in Yaworsky *et al*'s work regarding how ethical data practices can be employed in the expanding field of AI and big data to diminish data exploitation and the dangers of data breaches that could be exploited by malicious actors.

Cali *et al*[119] point out that due to the lack of robust consumer protection laws and low levels of financial literacy in developing nations like Kenya, combined with the rapid growth of FinTech, challenges such as consumers being overly indebted or encountering predatory lending practices may arise, as observed in Cali *et al'*s study on the potential consequences of these issues. They also state that the expansion of DFS could heighten macro-financial risks, which have not been adequately addressed through legislation.[120] They cite the case of Tanzania, where an interactive Short Messaging Service (SMS) system focusing on financial literacy content contributed to positive changes in the saving and borrowing habits of smallholder farmers.[121] This research highlights a gap in the examination of the digital infrastructure and capacity building's impact on DFS. This proposed study seeks to address this gap by assessing the possibility of a framework for regulating the rapidly evolving digital infrastructure to benefit consumers.

The International Telecommunication Union (ITU)[122] observes that data is becoming increasingly important to mobile financial services and that data, and its management are also key to profitability, and as a result, it is valuable. Furthermore, while delving into how digital activity leaves vast 'data exhaust' that can be useful in evaluating risk and reducing costs of lending and insurance, the ITU observes that control over access to such data is an important commercial and regulatory policy issue.[123] The research further states that data about a customer's revenue and expenditure habits enables the lender to assess the risk of the customer defaulting on the loans. Such data allows the lender to determine better on what terms to provide the loan on.[124] This research clearly indicates a gap in research on the glaring violation of data use and, with the application of AI, what the potential effects shall be on consumer data protection.

[118] Yaworsky *et al, Unlocking the Promise of (Big) Data to Promote Financial Inclusion,* 29-33.
[119] ibid (n 4) 96.
[120] ibid (n 4) 96.
[121] ibid (n 4) 96.
[122] ibid (26) 43.
[123] ibid (26) 44.
[124] ibid (26) 45.

Izaguirre and Mazer[125] observe that the significant increase and adoption of digital credit have led to elevated levels of default and delayed payments in Kenya, particularly among those living in poverty. The research delves into the pattern of borrowing in the Kenyan context but leaves a gap regarding the impact of consumer data on the high interest rates received by consumers and its effect on their repayment rates, as well as the failure of the informed consent model to shield consumers from predatory practices like these. The proposed research attempts to reduce this gap through its interrogation of the adequacy of the informed consent model in the law governing consumer data protection in DCSs.

Ezrachi and Stucke [126]have noted that price discrimination could be observed within the DFS industry noting that this happens when a company charges different prices to different consumer groups for identical or similar goods or services, not based on the cost of supply. Ariel and Maurice further argue that second-degree price discrimination, which refers to varying prices charged to buyers based on the quantity or quality of the purchased goods or services, is also possible in the DFSs.[127] In the context of DCSs, the buyers are the borrowers, and the quality is linked to whether they have previously defaulted on a credit facility, impacting the interest rates for loan facilities.[128] They observe that consumer data regarding defaults, readily accessible from the Credit Reference Bureau (CRB), as well as their text messages and any other information obtainable from their mobile phones, can easily be applied to discriminate against consumers through customised differential pricing harmful to competition.[129] While the study speaks to the concerns flagged by the proposed study as part of the problem, it does not do so in the context of Kenya, hence leaving a gap that the proposed study seeks to reduce.

1.9 Research Methodology

The research design adopted in this study is a doctrinal legal research approach because it relied solely on primary and secondary legal data mostly sought out through desk-based research. The secondary data was largely be derived from legislation, books, book chapters, credible institutional reports, peer-reviewed journal articles, treaties, and judicial decisions. The research also gleaned some secondary data from credible Newspapers for anecdotal

[125] Juan Carlos Izaguirre, and Rafe Mazer, *How Regulators Can Foster More Responsible Digital Credit,* (CGAP, November 2018).
[126] Ariel Ezrachi and Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge, MA: Harvard University Press, 2016) 85-89.
[127] ibid (n 124) 85-89.
[128] ibid (n 124) 85-89.
[129] ibid (n 124) 85-89.

information. Legislation and judicial decisions from Kenya were sought from online repositories such as the Kenya Law Reports (KLR) website, and foreign legislation and judicial decisions were sourced from credible websites. Treaties were also be sourced from the associated websites such as the United Nations (UN), European Parliament (EP) and European Council's (EC) website. The reports were sourced from online repositories such as the Strathmore Online Library catalogue as well as the Kenya National Library. Newspapers were sought from the paper's website, such as the Standard and Daily Nation; if they are unavailable, they will be sourced from the Kenya National Library and the Kenya Archives.

The use of multiple jurisdictions within this study is to understand the different contexts surrounding the various consent models. The EU is a foremost jurisdiction when it comes to the use and implementation of data protection systems, the General Data Protection Regulation (GDPR) has shown itself to be a shining example of how a state or a region should protect its people's data. Kenya's Data Protection Act is modelled from the GDPR; hence it would be of utmost importance to draw lessons while appreciating the unique and diverse contexts of both jurisdictions. South Africa has also shown itself as being a leading country in Africa in adopting and contextualising foreign actions, legislation and other aspects and tweaking them to their unique contexts. Kenya has a lot to learn about adapting foreign legislation and ensuring that it serves the Kenyan people in the most ideal manner possible.

1.10 Chapter Breakdown

The thesis is organised into five chapters. Chapter One is proposed to introduce the research problem and outline the methodology underpinning the study. Furthermore, it provides an overview of the theoretical framework underpinning the entire study. Additionally, it outlines the research objectives, limitations, and assumptions made in conceptualising this research topic.

Chapter Two is proposed to present the rationale, development, and scope of consumer data protection in digital credit services in Kenya. This chapter generally highlights the available consent models that have been applied in consumer data protection with a view to situating the informed consent model within the dominant discourse. The Chapter then interrogates the nature and scope of the informed consent model in depth from a conceptual point of view to build a basis for establishing its conceptual pitfalls. The chapter introduces the frontier technologies context that injects a disruptive variable in the larger ecosystem of consumer data protection.

Through detailed analyses and case studies, Chapter Three highlights the direct consequences and broader implications of regulatory frameworks on the development and growth of the DSP market in Kenya. Further, based on the conceptual grounding established in Chapter Two, Chapter Three locates the informed consent model as predominantly anchored in the existing framework on consumer data protection, including the Constitution of Kenya, 2010, the Consumer Protection Act, the Data Protection Act and the DCP Regulations. Chapter Three also evaluates the adequacy of the model as applied in these frameworks in governing consumer data protection in digital lending services. The research undertakes this evaluation while being mindful of the potential effects of frontier technologies such as Artificial Intelligence (AI) and blockchain technologies.

Chapter Four seeks to establish potential lessons from other jurisdictions on the issue of models for consumer data protection relevant to digital credit services. More particularly, the chapter seeks to draw lessons from the European Union (EU), the United States of America (USA), and South Africa. The analysis seeks to establish whether and how best practices from these jurisdictions can be applied to the Kenyan context despite considering variances in socio-economic, legal, and political contexts.

Chapter Five concludes the proposed study and presents a summary of research findings as arrived at from the preceding substantive Chapters of the thesis. Based on the findings, the Chapter highlights whether the hypothesis (together with its elements) has been proven or disproved and whether the research questions have all been answered. The Chapter also provides recommendations with respect to the governance of consumer data protection in digital credit services, including identifying opportunities for future research in the area.

CHAPTER TWO
CONCEPTUALISING CONSUMER DATA PROTECTION IN DIGITAL CREDIT SERVICES

2.1 Introduction

The rapid evolution of DFS, particularly DCSs, has revolutionised consumers' access to and availability of credit services.[130] However, as observed in the previous chapter, this rapid expansion has introduced new challenges to consumer data protection as data controllers and processors collect, process, and share vast amounts of personal and financial information.[131] Consumer data protection has become a critical aspect of DCSs due to the sensitive nature and value of the data collected.[132] Consequently, concerns about how this data is handled,[133] especially regarding consent, transparency, and accountability,[134] have become increasingly relevant.[135] This chapter aims to analyse the conceptual underpinnings of consumer data protection, focusing on the role of consent models within regulatory frameworks. It will further examine how different consent models function, their strengths and weaknesses, and the impact of global data protection legislation on DCPs and consumers.

This chapter is organised into five sections. First, the chapter provides a developmental background of key legislation and consent models. Next, key concepts such as informed consent, data privacy,[136] data protection and digital credit services will be discussed in relation to these frameworks. Informed consent plays a pivotal role in data protection since it governs the extent to which consumers knowingly allow their data to be used for specific purposes. Lastly, this chapter explores how these principles influence both current practices and future trends in consumer data protection, and provides a conclusion based on the foregoing findings.

---

130 John Babikian, *Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era*, (Law Research Journal, Vol 1, No 2, January 2023), 91.

131 Omar Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, (Northwestern Journal of Technology and Intellectual Property, Vol 11, No 5, April 2013), 240.

132 Omar Tene *et al*., *Big Data for All: Privacy and User Control in the Age of Analytics,* (n 129) 240.

133 Ryan Calo*, Digital Market Manipulation*, (George Washington Law Review, Vol 82, No 4, 2014) 998.

134 Helen Nissenbaum, *A Contextual Approach to Privacy Online*, (n 19), 34.

135 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 242.

136 Helen Nissenbaum*, A Contextual Approach to Privacy Online,* (n 19) 33.

2.2 Rationale for Consumer Data Protection in Digital Credit Services

In DCSs, protecting consumer data is viewed as a panacea, driven by mounting concerns over privacy violations and data misuse.[137] Different consent models have been developed and implemented to safeguard personal data. These include explicit consent, where consumers must actively agree to data processing; implicit consent, where data is collected through passive means; and informed consent, where consumers are assumed to be fully informed about how their data will be used before, they give permission.[138]

DCS, driven by advanced algorithms, AI and ML, has access to diverse data, including behavioural, demographic, and financial information. This data can be monetised or utilised to influence consumer behaviour without their explicit knowledge or consent. Additionally, the increasing application of AI and ML for assessing consumer creditworthiness, tracking repayment behaviours, and customising financial products underscores the urgent need for consumer data protection.[139] The digital nature of these services further heightens consumers' vulnerability to data breaches, unauthorised access, data sharing, and misuse, thus necessitating the implementation of robust protection frameworks.[140] The types of data collected encompass mobile phone usage, social media activity, and location information, extending far beyond traditional credit-scoring methods.[141] This extensive data collection reinforces the need for stringent data protection measures to safeguard consumer rights, privacy, and financial security. Many consumers remain unaware of the full extent of the data being gathered and its potential applications, rendering them susceptible to privacy violations.[142] It is, therefore, essential to ensure that consumers retain control over their data and comprehend how it is utilised, as this is crucial for protecting their rights and promoting a fair digital credit landscape.[143]

2.3 Development of Consumer Data Protection in Digital Credit Services in Kenya

Historically, the development of data protection laws can generally be traced to the 1980 emergence of the Organisation for Economic Cooperation and Development (OECD)

---

137 Oluwatosin Reis, Nkechi Emmanuella Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, and Temitayo Oluwaseun Abrahams, *Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement*, (International Journal of Applied Research in Social Sciences, Vol 6, Issue 1, 2024), 73.

138 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 261.

139 Oluwatosin Reis, *et al.*, *Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement*, (n 135) 78.

140 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 251.

141 ibid (n 129) 260.

142 ibid (n 129) 251.

143 ibid (n 129) 260.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[144] It has been argued that these guidelines laid the foundation for modern data protection frameworks generally.[145] While the OECD Guidelines may have marked the formative origins of data protection frameworks generally, the subsequent adoption of the EU GDPR in 2016 may arguably be seen as the trigger for a race towards data protection across the globe.[146] This was the case as many countries commenced the debate on whether and how to establish data protection legal regimes generally – a debate that saw various countries enact data protection laws in steady succession thereafter, including the enactment of Kenya's Data Protection Act (DPA) in 2019 as a *sui generis* data protection regime aligned to Kenya's context. Perhaps this resonated with the import of context for data protection, as argued for by Nissenbaum through her extensive work on contextual integrity,[147] in which she observes that data protection must align with the context in which the data was originally shared, thus effectively influencing legislation to balance consumer rights offline and online.

A better understanding of the context of the DPA can be gleaned from the *travaux preparatoire* on this issue, which includes parliamentary discussions that considered the Data Protection Bill in October 2019. A Hansard Report on the consideration of the Bill[148] - now the Data Protection Act – indicated that the proposed Act was meant to give effect to the right to privacy as enshrined in Article 31 of the Constitution of Kenya, 2010.[149] The executive summary of the memorandum accompanying the Bill cited, *inter alia*, that data subjects had the right to be informed of the purposes for which their personal data is to be used.[150] Through this requirement, Parliament had the benefit of considering and providing for informed consent to private data handling, which it did, as evidenced by the ultimate DPA as assented to. While Chapter Three of this thesis discusses the relevance of the DPA for the problem subject of this study in greater detail, the objects and purpose of the Bill are noteworthy as these signal the scope of protection. The objects and purpose of the Bill, as later replicated in the DPA, included regulating the handling of personal data and ensuring the lawful management of such data in line with the principles of legitimate processing. The objectives of the Bill also included establishing legal and institutional frameworks to protect personal data and granting data

144 John Babikian, *Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era*, (Law Research Journal, Vol 1, No 2, 2023) 94.
145 ibid (n 142) 94.
146 ibid (n 142) 94.
147 Helen Nissenbaum*, A Contextual Approach to Privacy Online,* (n 19) 34.
148 National Assembly Hansard Report, 17 October 2019, 6.
149 National Assembly Hansard Report, 17 October 2019, 6.
150 National Assembly Hansard Report, 17 October 2019, 6.

subjects rights and remedies related to safeguarding their personal information.[151] The Bill, passed into DPA, formed the substantive and procedural scope of data protection specifically applied to data protection in DCSs (a phenomenon discussed substantively in Chapter Three of this thesis).

Indeed, the ultimate assent to the DPA marked a milestone in the development of Kenya's consumer data protection laws.[152] The DPA was developed in response to mounting concerns about the unregulated use of personal data. These concerns were particularly reflected in cases where consumers often lacked sufficient knowledge of how their data would be used, applied or shared, hence undergirding the import of informed consent.

Even more relevant to the context of considering data protection law applicable to DCSs is the prominent participation of the Digital Lenders Association of Kenya (DLAK), which was heavily involved in public participation in respect of the Bill leading to DPA.[153] Notably, DLAK opposed the provisions of the Bill that required the Office of the Data Protection Commissioner (ODPC) to register data controllers and processors.[154] While it may be argued that this proposal may have reflected the sentiments of DLAK's members to reduce the scope of regulation applicable to DCPs, this has subsequently been disproved, as the ODPC has been registering and maintaining a register of all data controllers and processors in Kenya with minimal, yet surmountable, challenges.[155] Had the DLAK recommendation been implemented, the ODPC would have rendered its regulatory powers impractical as registration has, over time, provided a framework for the ODPC to monitor and enhance compliance in data handling by the registered entities. Instead, the proposal would have largely meant DCPs largely out of the ODPC's regulatory reach. In sum, these developments have meant that consumer data protection within the realm of DCSs is covered.

The development of consumer data protection in DCSs in Kenya was not without some key drivers worthy of note at this point. To start with, the rapid rise of DCS fundamentally altered the credit landscape, particularly in emerging markets such as Kenya, where mobile money platforms like MPesa and a proliferation of digital lenders, as highlighted in Chapter One, have

---

152 The Data Protection Act, 2019 was assented to on 8 November 2019 and commenced on 25 November 2019.
153 National Assembly Hansard Report, 17 October 2019, 16.
154 National Assembly Hansard Report, 17 October 2019, 21.
155 Office of the Data Protection Commissioner, *Registered Data Handlers,* Registered Data Handlers - Office of the Data Protection Commissioner (ODPC) accessed on 19th February 2025.

been expanding financial inclusion over the years.[156] This shift towards digital credit was generally partially facilitated by an inviting regulatory landscape and the integration of advanced technologies like AI and ML, big data analytics and blockchain.[157] These innovations allow DCPs to assess consumers' creditworthiness more efficiently by leveraging the vast amounts of consumer data collected.[158]

In addition, the growing digital literacy of consumers, coupled with the demand for financial services and the proliferation of mobile and internet technologies, has - over the years - influenced the continuous development of consumer data protection. DCPs, which initially operated in an unregulated environment, are now subject to closer - yet not optimal - scrutiny as the evidence seems to suggest a recognition of the importance of continuous improvement in protecting consumer data with the deepening of frontier technologies. This further highlights the growing understanding of the value of data in a digitising economy and the need to protect the consumer.

While the developments in DCSs have seemingly improved access to credit, they have also raised major concerns about data privacy generally, particularly for consumer data and information protection. Some of the concerns continue to challenge the scope of consumer digital protection in Kenya.

2.4 Scope of Consumer Data Protection in Digital Credit Services in Kenya

The scope of consumer data protection within DCSs in Kenya is extensive, covering a variety of activities that include the initial collection of data, its subsequent processing and storage, and its eventual deletion or transfer to third parties.[159] Thus, it is crucial to underscore the importance of securing consumers' control over their data and privacy throughout its lifecycle. The collective various aspects of the lifecycle include data collection, data processing and analysis, data storage and retention, data sharing and transfer, as well as consumers' rights and remedies. This collective, as per the argument of this thesis, is not only conceptually

---

156 Kevin Donovan, *Mobile Money for Financial Inclusion*, (Mobile Money for Financial Inclusion, Information and Communications For Development) 81. See also; Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics,* (n 129) 254.

157 Oluwatosin Reis, *et al.*, *Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement*, (n 135) 78.

158 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytic*s, (n 129) 252, 253.

159 John Babikian, *Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era*, (n 142) 94.

appreciated but also catered for, though not conclusively, in the consumer data protection regime applicable to DCSs in Kenya.

2.4.1 Collection of Consumer Credit and Related Data

DCSs rely on the collection of vast amounts of data to assess consumers' creditworthiness and manage lending risks.[160] This data may include some traditional financial information, such as the borrower's income, spending habits, and loan repayment history. Moreover, increasingly, it also includes non-financial data, such as mobile phone usage, social media activity, and the borrowers' geolocation data.

DCPs in Kenya, such as Tala and M-Shwari, collect consumer data through their mobile platforms, allowing consumers to apply for loans using their mobile phones. The scope of consumer data protection requires that lenders collect only the data necessary for credit evaluation[161] and that consumers are aware of its collection and purpose of use.[162] The Data Protection Act imposes limits on the types of data that can be collected and mandates that personal data should only be collected for specific and legitimate purposes.[163] It remains questionable whether this provision is complied with in view of the data collected through Intelligent Agents (IAs) within the frontier technologies.[164] While the collection of data is necessary and justified for the purpose of granting loans to consumers, there is a major risk of the DCPs collecting data unrelated to the purpose for which the consumer has granted consent as well as the data being utilised for purposes unrelated to the purpose consented to.

2.4.2 Processing and Analysis of Consumer Credit Data

After data collection, the information within the DCS undergoes processing and analysis by an algorithm to assess the creditworthiness of the consumer(s). This process commonly employs advanced and highly sophisticated algorithms, along with machine learning models, to predict the likelihood of loan repayment or default by identifying patterns within the consumer's data.[165] The handling of data must adhere to the essential principles of fairness, transparency,

---

160 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytic*s, (n 129) 252.

161 Helen Nissenbaum, *A Contextual Approach to Privacy Online*, (n 19)34.

162 Data Protection Act, 2019, 2019, s 29 (g).

163 Data Protection Act, 2019, 2019, s 29 (g).

164 Data Protection Act, 2019, 2019, s 29 (g). See also; Kanerika, *AI Agents in Finance: A New Era of Efficiency and Innovation*, (December 29, 2024). AI Agents in Finance: Role, Benefits, and Future Trends accessed on 12th February 2024.

165 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 243. See also; Erik Brynjolfsson, Lorin Hitt and Heekyung Kim, *Strength in Numbers: How Does Data-Driven Decision-Making Affect Firm Performance?,* (No 5, April, 2011), 242.

and accountability. This means that all data processing activities should be conducted with an impartial approach, ensuring that individuals are not discriminated against or treated unjustly. Transparency requires that the processes involved in data collection and usage are clear and open, allowing individuals to understand how their information is being utilised and for what purposes. Additionally, accountability necessitates that organisations are responsible for their data practices, being prepared to explain their actions and address any concerns or grievances arising from data processing.[166]

Nonetheless, with the advent of the black-box effect - a phenomenon where the inner workings of a system become obscured or opaque - these foundational principles become increasingly challenging to adhere to. This complexity arises because the lack of transparency makes it difficult to understand how decisions are made or assess the underlying processes' reliability, complicating our ability to apply established guidelines effectively.,[167] let alone enforce them.[168] While the DPA requires that data processing be lawful and consumers be informed of how the data will be processed and used, it raises the question of what happens when the data processing becomes opaque, even to the DCP.[169]

In Kenya, the integration of big data and artificial intelligence into the credit scoring process has sparked significant discussions about the transparency and fairness of the algorithms used.[170] As financial institutions increasingly rely on these technologies to assess creditworthiness, questions arise regarding how data is collected and analysed and the potential biases that may exist within the algorithms. Stakeholders are concerned that certain groups may face discrimination or unequal access to credit without clear insights into the decision-making processes and underlying data sources. Furthermore, the complexities of these algorithms can make it difficult for both consumers and regulators to challenge or understand the outcomes of credit assessments, highlighting the need for greater accountability and ethical considerations in the deployment of these advanced analytical tools.[171] Algorithms can be susceptible to reinforcing the biases of the system's creator(s) or user(s).[172] Such biases can – and frequently do – result in unjust lending outcomes, especially impacting marginalised communities and

166 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 242.
167 Oluwatosin Reis, *et al.*, *Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement*, (n 135) 76.
168 ibid (n 129) 243.
169 ibid (n 129) 244.
170 Oluwatosin Reis, *et al.*, *Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement*, (n 135) 76.
171 ibid (n 135) 76.
172 ibid (n 129) See also, Ryan Calo, *Digital Market Manipulation*, (n 131) 1001.

individuals in less developed areas of the country. This adds to the previously mentioned black box effect. When examined together, the consequences of unregulated AI and the use of big data appear to present a troubling aspect overshadowing any potential benefits.

2.4.3 Data Storage and Retention in Respect of DCSs

Under the Data Protection Act,[173] Data controllers and processors are responsible for implementing appropriate technical and organisational measures to safeguard personal data. This is crucial to protect against incidents such as accidental or unlawful destruction, loss, alteration, and unauthorised disclosure or access. The significance of robust data security is particularly pronounced in sectors involving consumer data protection, such as DCS, where there is a heightened risk concerning individuals' sensitive financial information and personal data.

In parallel with securing data, these entities also need to adhere to prudent data retention practices. Specifically, data controllers and processors should retain personal data only for the duration necessary to fulfil the purpose for which it was originally collected.[174] This means that a clear retention policy must be established for all retained data, including stipulations about how long each category of data will be held. This policy should remain in effect even if the data subject ceases to utilise the service provided.

The data retention periods should be explicitly detailed within the privacy policy to ensure transparency.[175] This allows consumers to be well-informed about how long their data may be retained and under what conditions it might be deleted. Moreover, data subjects possess the right to request the deletion of their personal data when they terminate their use of the service or deem the data irrelevant for its intended purpose.

During the retention period, data subjects should also be empowered to modify or correct any inaccuracies in their data.[176] This capability is essential, as it helps maintain the integrity and accuracy of the data held by data controllers and processors. By addressing these aspects of data security and management, organisations can build a more trustworthy relationship with consumers, ultimately fostering greater confidence in handling their personal data.[177]

---

173 Data Protection Act, 2019, s 29.
174 Data Protection Act 2019, s 39
175 Data Protection Act, 2019, s 39 (2).
176 Data Protection Act, 2019, s 40.
177 Zlatan Moric, Vedran Dakic, Daniela Djekic and Damir Regvart, Protection *of Personal Data in the Context of E-Commerce*, (Journal of Cybersecurity and Privacy, Vol.4, September 2024), 753.

2.4.4 Data Sharing and Transfer

The exchange and transfer of consumer data to third parties have become a highly contentious issue within DCSs. Many DCPs engage in practices that involve selling or sharing consumer data with various entities, including other financial institutions, marketing agencies, and even data brokers.[178] This often occurs without obtaining explicit consent from the data subjects, which raises severe concerns regarding data privacy and security.

The ramifications of such practices are substantial, as the unauthorised sharing of personal information can lead to significant risks for consumers.[179] These risks include exposure to data misuse, identity theft, and fraud, all of which can have devastating effects on an individual's financial stability and personal security.[180] Furthermore, this lack of transparency in data handling practices contributes to a growing distrust among consumers regarding how their information is managed and protected, highlighting the urgent need for more stringent regulations and better data governance to safeguard consumer rights.[181]

Aside from requiring explicit consent prior to data sharing and transfer, the Data Protection Act restricts cross-border data flows to ensure adequate data protection. This is critical particularly where the DCP's servers are hosted outside Kenya. A similar position has been adopted in the EU where in *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Consteja Gonzalez (Google Spain Case*).[182] The Court of Justice of the European Union (CJEU) decided that a search engine's activity should be classified as processing personal data when the information contains personal data, and the operator of such processing must be considered a controller. A similar definition can be applied to DCPs collecting and processing consumer data.

2.4.5 Consumer Rights and Remedies

The Data Protection Act grants data subjects several rights against data handlers.[183] These rights are designed to empower consumers, permitting them greater control over their personal

---

178 Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals Threats to American Civil Rights, National Security, and Democracy,* (Dule Sanford, Cyber Policy Program), 2. See also; Federal Trade Commission, *FTC to Study Data Broker Industry's Collection and Use of Consumer Data* https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data accessed on 20th February 2025.

179 Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals Threats to American Civil Rights, National Security, and Democracy,* (n 176) 2.

180 ibid (n 176) 2.

181 ibid (n 176) 2.

182 Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Consteja Gonzalez (Case C-131/12).

183 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 1880.

data and providing mechanisms for redress in cases of misuse or data breaches. First, the right to access.[184] According to section 26(b) of the DPA, consumers have the right to request access to their personal data held by data handlers, specifically the DCP. This right includes inquiries about how their data is being utilised, to whom it has been shared, and for what purposes.

Second, the right to correction.[185] According to Section 26 (d) of the DPA, consumers have the explicit right to request the DCP to amend any data they consider to be inaccurate or outdated. Alternatively, the DCP must provide a means for such amendments. This is particularly crucial in DCS, as inaccurate data can result in algorithmic bias, which in turn may lead to flawed credit assessments and unfair lending decisions.186

The third of consumer rights is the right to deletion. Under Section 26(e) of the Data Protection Act, consumers have the explicit right to request the deletion of their data when it is no longer necessary for the purpose for which it was collected. This often occurs when a consumer decides to withdraw from a lending application and wishes for their data to be deleted and not retained or shared further. The European Commission proposed the right to be forgotten, which has been incorporated into the General Data Protection Regulation (GDPR).[187]

Fourth, the right to object to data processing. The Data Protection Act (DPA), specifically under Section 26 (c), establishes the right for consumers to object to specific types of data processing activities. This provision is particularly relevant in cases where the processing of their personal data is deemed unlawful or when it poses a substantial risk to their privacy. Consumers are empowered to express their concerns and request that such processing be halted, thereby protecting their personal information from misuse and ensuring that their rights are respected in handling their data.

The fifth right is the right to data portability.[188] Section 25 of the DPA clearly establishes the right to data portability. This provision allows consumers to transfer their personal data from one DCP to another seamlessly. By enabling this transfer, the Act promotes competition among DCPs, ensuring that no single provider can monopolise the market. This mechanism serves to prevent scenarios where consumers might feel trapped with one DCP due to constraints imposed by data restrictions. As a result, consumers are empowered to make informed choices

184 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 252.
185 ibid (n 129) 252 .
186 Ryan Calo*, Digital Market Manipulation*, (n 131) 1001.
187 ibid (n 129) 252.
188 ibid (n 129) 263.

about their services, fostering an environment of innovation and competition within the digital landscape.

2.5 An Overview of Consent Models Relating to Consumer Data Protection

Consent is a fundamental concept to any data protection regimen as it provides legal and regulatory basis for collecting and processing personal data.[189] Ensuring consent is meaningfully obtained is essential for maintaining trust between consumers and DCPs. Similarly, without robust mechanisms, consumers remain vulnerable to data misuse. The importance of consent is emphasised in international data protection frameworks, such as GDPR and the Data Protection Act.

Consent models are integral to data protection frameworks since they dictate how consumers authorise collecting, processing and sharing their personal data. The most common consent models include opt-in and opt-out, implicit, and informed consent. In DCS, consent models are often scrutinised for their effectiveness in ensuring consumers fully understand the implications of sharing data. The adequacy of these models is heavily debated, as indicated in this study, with informed consent often being assumed as the most robust yet difficult to implement effectively due to its complexity. The models vary in terms of control and understanding they offer to the consumer.

2.5.1 Informed Consent Model

In this context, a comprehensive benchmark for consumer data protection is established, particularly informed by the Data Protection Act (DPA) provisions. Central to the DPA is the principle of obtaining informed consent, which is recognised as a fundamental prerequisite for any lawful data processing activities. This means that organisations seeking to collect and process personal data must ensure that consent is obtained only after individuals have received thorough information regarding a multitude of factors. These factors include, but are not limited to, the specific purposes for which their personal data is being collected, the nature and scope of the data processing activities that will occur, and the rights that are afforded to them as data subjects under the Act.[190] A key strength of this model is its emphasis on transparency and consumer empowerment; however, its practical effectiveness is heavily reliant on how clearly and effectively the information is communicated to consumers.

---

189 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 260.
190 Helen Nissenbaum, *A Contextual Approach to Privacy Online,* (n 19) 34.

In practice, the implementation of these requirements often encounters significant challenges. Many privacy policies and terms of service documents are characteristically lengthy and filled with complex legal language, which can create barriers to understanding.[191] Due to this convoluted presentation, consumers may struggle to grasp the essential terms and conditions they are agreeing to, ultimately undermining the core principles of transparency and empowerment that the DPA model seeks to promote.

Enhancing the clarity and accessibility of such documentation is crucial to better align with the ideals of informed consent. This can involve simplifying legal language, breaking down information into easily digestible formats, and adopting user-friendly design principles. By doing so, organisations can ensure that consumers are aware of their rights and the implications of data sharing and feel genuinely empowered to make informed choices regarding their personal information, thus fostering a more effective and robust data protection environment.[192]

2.5.2 Dynamic Consent Model

This emerging model allows consumers to consent continually, allowing for more flexibility and responsiveness on how their data is used. It is important where data collection and use evolve. Unlike traditional consent models, where consent is typically given once at the beginning of a transaction, this model recognises that data processing activities may change over time and provides the consumers with the continuous ability to manage their consent.

This model is flexible and responsive to the needs of the consumers, highlighting its major strength. It offers a more consumer-centric approach to data protection by allowing real-time data management by the consumer(s). Its challenge, however, lies in the technological infrastructure required to support its full implementation. DCPs would need to invest in systems that allow for real-time updates to consent preferences which are perceived to be costly and complex to manage.

2.5.3 Implied Consent Model

The implied consent model is based on the principle that consumers grant permission through their actions rather than through explicit agreements.[193] For example, when a user interacts with a digital service - such as downloading an app, browsing a website, or subscribing to an

---

191 ibid (n 19) 34.

192 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, (n 32) 1881.

193 Intersoft Consulting, *GDPR Consent,* (July 2023) https://gdpr-info.eu/issues/consent/ accessed on 18th February 2025 See also; Securiti, *What are the Different Types of Consent?*(July 2023) https://securiti.ai/blog/types-of-consent/ accessed on 18th February 2025

online platform - they are often considered to have provided implicit consent for their data to be collected and utilised in accordance with the service's terms.

This model starkly contrasts opt-in approaches, where users must take definitive action - like checking a box or clicking a confirmation link - to indicate their agreement to the data processing terms.[194] While the implied consent model can enhance user experiences by minimising interruptions, such as pop-up requests for consent, it raises significant concerns regarding consumer awareness and data privacy.

One major risk associated with this model is that consumers may not fully understand or be aware of the extent to which their personal information is collected, processed, and potentially shared with third parties.[195] This lack of transparency can lead to scenarios where users are uninformed about how their data is utilised, thereby increasing the likelihood of misuse or exploitation.

Additionally, regulatory frameworks like the Data Protection Act underscore the importance of obtaining explicit consent from individuals before processing their personal data. These laws are designed to protect consumer privacy and ensure that individuals are well-informed and have control over the usage of their data. Consequently, the use of implied consent models may be less advantageous and could present challenges in jurisdictions with stringent data protection regulations, which often prioritise informed consent as a key principle in data handling practices.

2.5.4 Opt-in Model

The Model necessitates clear consent from consumers for the use of their data, typically achieved by either checking a box or signing a document. It is frequently regarded as the gold standard since it guarantees that consumers are fully informed about and have consented to data collection and processing prior to its occurrence.[196]

The GDPR follows an opt-in approach. According to the GDPR, businesses are required to secure explicit and informed consent from individuals before collecting and processing their

---

194 Elisabeth Hildt and Kelly Laas, *Informed Consent in Digital Data Management,* (Illinois Institute of Technology, January 2022), 7. Intersoft Consulting, *GDPR Consent,* (July 2023) https://gdpr-info.eu/issues/consent/ accessed on 18th February 2025 See also; Securiti, *What are the Different Types of Consent?*(July 2023) https://securiti.ai/blog/types-of-consent/ accessed on 18th February 2025.

195 Intersoft Consulting, *GDPR Consent,* (July 2023) https://gdpr-info.eu/issues/consent/ accessed on 18th February 2025 See also; Securiti, *What are the Different Types of Consent?*(July 2023) https://securiti.ai/blog/types-of-consent/ accessed on 18th February 2025

196 Helen Nissenbaum, *A Contextual Approach to Privacy Online, (n 19)*35.

personal information. This indicates that consumers must actively consent to data collection by giving approval that is freely given, specific, informed, and clear. The GDPR also mandates that data handlers offer consumers transparent information regarding how their data will be utilised, and consumers have the irrevocable right to withdraw their consent at any point. Additionally, the GDPR places significant importance on data minimisation.[197] – where only the most necessary data should be collected, and data handlers must implement privacy by design and by default.[198] Under the DPA, explicit consent is a legal requirement for the processing of personal data. In DCS this may include but is not limited to the consumer's financial history, mobile phone usage patterns and even their location data.

This consent model has the strength of transparency, and the active participation required from consumers.[199] In Kenya, data controllers and processors, including DCPs, have a crucial responsibility to provide detailed and transparent explanations regarding the reasons for collecting personal data. This practice aims to significantly reduce the likelihood of unauthorised use of individuals' private information. However, a key limitation of this approach is the uncertainty surrounding whether consumers genuinely grasp and understand the information being conveyed to them.[200] Many consumers frequently find themselves agreeing to terms and conditions without thoroughly reading or comprehending the content. This tendency is particularly prevalent when the agreements are extensive, filled with legal jargon, or presented in a complex manner. The length and technical language can create barriers for individuals who may not have the time or expertise to parse through the dense information, leading to a situation where consent is given without a full grasp of the implications involved. As a result, consumers may unwittingly agree to conditions that could significantly affect their rights and obligations.[201] The prevalence of consent fatigue further aggravates the issue.[202]

2.5.5 Opt-out Model

The model in question is based on the premise that consent is automatically assumed unless consumers actively take steps to opt-out. This perspective poses substantial challenges for DCS, as many consumers may not fully grasp that their personal information is being collected and utilised unless they explicitly indicate their desire to opt-out. Consequently, this default

197 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics,* (n 129) 259.
198 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, (n 32)1889.
199 ibid (n 32)1888.
200 ibid (n 32)1883.
201 ibid (n 32)1885.
202 ibid (n 32)1888.

assumption places the responsibility of safeguarding data rights squarely on consumers. They must navigate intricate privacy policies and various data collection practices without clear guidance, which heightens the risk of unintentionally relinquishing control over their personal data. This situation underscores the urgent need for more transparent practices and proactive initiatives to educate consumers about their data rights and the implications of their consent.[203] Some DCPs have employed this model in Kenya, assuming that using a service means consenting to data collection.

This situation is especially concerning as it often fails to provide consumers adequate notification or clarity regarding how their personal data is processed.[204] Many individuals may be unaware that their data is being collected unless they actively seek out and carefully review the privacy policies of the services they use. This lack of transparency can leave consumers uninformed about how their information is managed, leading to significant privacy concerns and issues of trust.

The DPA underscores the importance of obtaining explicit consent from individuals before collecting their personal information.[205] However, in the Kenyan market, implicit consent models are not only present but also widely practiced. This situation arises, in part, due to the insufficient regulatory oversight of DCPs. As a result, consumers often find themselves in a position where they must proactively opt out of data collection activities. This can be a significant challenge, particularly for individuals who may lack the essential digital literacy required to effectively navigate the intricate privacy settings that companies employ. Such complexities can leave vulnerable populations at risk of having their personal information harvested without their informed agreement.[206]

Despite its drawbacks, it offers a seamless user experience with fewer interruptions from consent requests. However, a notable limitation of this approach lies in the core principle of informed consent, which assumes that consumers are aware of and have automatically agreed to data processing. This assumption makes the model increasingly less appealing and inadequate for consumer data protection in data collection systems.

---

203 Helen Nissenbaum, *A Contextual Approach to Privacy Online, (n 19)*35.
204 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* (n 32)1883.
205 Data Protection Act 2019, s 26.
206 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* (n 32) 1884.

2.5.6 Granular Model

This model allows consumers to consent to different types of data processing individually, instead of giving a blank consent for all purposes.[207] This model is considered more consumer-friendly since it offers more control over which data can be collected and how it is used. An example could be consumers agreeing to provide their financial data for credit scoring purposes but refusing to share their location data for marketing purposes.

In Kenya's digital credit market, granular consent has the potential to significantly enhance consumer data protection. The Data Protection Act supports the principle of purpose limitation which aligns with this model.[208] The Act also requires that data controllers ensure that personal data is processed only for the purposes for which it was collected. Granular consent can operationalise this principle by allowing consumers to choose which specific data they are willing to share for which purposes.[209] This indicates that the Act proposes multiple types of consent models.

Its strength lies in its ability to give consumers more control and autonomy over their data. It empowers consumers to make informed decisions about collecting, processing, and using their data. However, a challenge lies in its complexity. The offer of multiple consent models may overwhelm consumers, leading to either confusion or disengagement.[210] For DCPs, implementing this model requires more sophisticated systems and processes that may require increased costs.

Despite the apparent drawbacks, this model has been considered a future-forward model aligned with the global push towards more transparent and consumer-centric data protection practices. In Kenya, where the consumer base is increasingly educated and becoming more aware of their data rights, this consent model has the opportunity to play a critical role in strengthening consumer data protection in DCS.

2.6 Situating the Informed Consent Model in the Consumer Data Protection

In the rapidly evolving digital landscape, consumer data protection has become a crucial issue, particularly regarding DCSs in Kenya. As data collection techniques advance, the urgency for robust data protection frameworks grows. A key element within these frameworks is the

---

207 ibid (n 32) 1885.
208 Data Protection Act 2019, s 29 (c).
209 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Version 2.0, October 2020), 9.
210 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* (n 32) 1885.

principle of informed consent, which aims to empower consumers by ensuring they clearly understand how their data is utilised. This model, founded on the principles of transparency, autonomy, and accountability, seeks to bridge the divide between consumers and data controllers, fostering trust and promoting informed decision-making.[211] However, implementing the informed consent model in Kenya encounters distinct challenges and opportunities, influenced by the country's specific regulatory landscape and citizens' digital literacy levels.

2.6.1 Conceptualising the Informed Consent Model

The informed consent model is fundamentally based on the principle that consumers should possess a comprehensive understanding of various aspects concerning the data being collected about them. This includes a clear explanation of the type of data being gathered, the specific purposes for which it will be utilised, and the potential risks and implications associated with its collection and processing. The objective of informed consent is to ensure that individuals receive adequate information that is not only factual but also presented in a way that is accessible and comprehensible to a wide audience.

This model aims to uphold several core principles: autonomy, which empowers consumers to make informed decisions about their personal data; transparency, which calls for openness regarding data practices; and accountability, ensuring that entities collecting consumer data are responsible for their actions and the consequences that arise from them.[212] Such principles are essential for fostering a sense of consumer trust and control over personal information in an increasingly data-driven world.

However, several significant factors severely challenge the informed consent model's practical effectiveness. One of the most pressing issues is the inherent complexity and often overwhelming length of privacy policies that consumers encounter.[213] Many individuals lack the time or motivation to read and understand these documents thoroughly, resulting in a superficial grasp of their implications.[214] Additionally, the technical intricacies involved in data collection and processing can be difficult for the average consumer to fully understand, further contributing to a knowledge gap.[215]

---

211 Elizabeth Hildt *et al., Informed Consent in Digital Data Management,* (n 192) 7.
212 ibid (n 192) 7.
213 ibid (n 192) 20.
214 ibid (n 192) 16.
215 ibid (n 192) 20.

Moreover, a pronounced power and information asymmetry exists between consumers and DCPs. Consumers typically find themselves at a disadvantage, with limited negotiating power and access to relevant information, which undermines their ability to provide truly informed consent.[216] This idealised model of informed consent ultimately faces significant hurdles in its implementation, highlighting the need for further reforms and solutions that prioritise consumer rights and understanding in the digital age.[217]

Transparency is a fundamental principle in data protection frameworks like the GDPR and POPIA which require companies to disclose how data is collected, processed, and shared.[218] It attempts to ensure that consumers make or can make informed decisions regarding whether or not to engage with DCS.

Transparency is closely tied to accountability, which refers to organisations' responsibility to demonstrate compliance with data protection standards, such as protecting data in transit or at rest.[219] Data audits and third-party assessments are some of the critical mechanisms in ensuring proper accountability.[220] However, this is demonstrably difficult when it comes to cross-border data flows due to the differing legal requirements and compliance efforts between jurisdictions.

2.6.2 Informed Consent Model in Consumer Data Protection in DCSs

The informed consent approach is of paramount importance, particularly given the extensive data collected for credit evaluation purposes. Consumers may not always be aware that their information is being amassed from a variety of digital activities.[221] The evaluation of an individual's financial behaviour is a multifaceted process that integrates various data sources to create a comprehensive financial profile. In addition to traditional financial metrics, such as credit scores, income, and existing debts, the analysis now incorporates elements like social media activity, which can offer insights into lifestyle choices and spending habits.

Browsing patterns are also examined, as they can reveal consumer interests and purchasing intentions.[222] Mobile phone usage data further enhances this understanding, as it provides information on communication habits and app usage relevant to financial management.

---

216 ibid (n 192) 17.
217 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics*, (n 129) 243.
218 ibid (n 129) 270.
219 Elizabeth Hildt *et al., Informed Consent in Digital Data Management,* (n 192) 17. See also Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics,* (n 129) 270.
220 Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics,* (n 129) 270.
221 ibid (n 19) 37.
222 ibid (n 19) 37.

Moreover, an individual's history with previous loans adds another layer of context, allowing for an assessment of repayment patterns and creditworthiness.

Importantly, biometric data - such as fingerprints, facial recognition, and other unique physical traits - are increasingly being utilised to enhance security and validate identity, ensuring a more accurate assessment. Together, these various data points create a richer, more nuanced picture of a person's financial behaviour, aiding in risk assessment and decision-making processes.[223]

The challenge lies in ensuring consumers are fully informed about the scope of data collection and the potential for data sharing with third parties including data brokers and advertisers.[224] Informed consent in DCSs is thereby not only about obtaining permission but also about fostering transparency and trust. In jurisdictions where data protection laws and their enforcement are robust, such as the EU and the United States of America (USA),[225] informed consent must be specific, unambiguous, and revocable. However, in many developing jurisdictions, including Kenya, the implementation of such standards is slow in its evolution, indicating significant gaps in consumer awareness and regulatory enforcement.

2.6.3 Conceptual Pitfalls in the Informed Consent Model

Despite its theoretical foundations, the informed consent model encounters several significant conceptual and practical challenges that undermine its effectiveness. A major concern revolves around the imbalance of power and information between consumers and organisations.[226] This disparity creates a situation where individuals often feel pressured and ill-equipped to make informed decisions about their own data.

One prominent consequence of this imbalance is a phenomenon known as consent fatigue. This occurs when users are bombarded with an overwhelming number of requests for consent, often presented in the form of lengthy and complex privacy policies that can be difficult to comprehend. As a result, many consumers reach a point of frustration or saturation, ultimately opting to click 'I Agree' without taking the time to fully parse the implications of the terms and

223 ibid (n 19) 38.
224 ibid (n 19) 38.
225 ibid (n 19) 39.
226 Daniel Outman, Rafe Mazer, Shana Warren, and William Blackmon, *Understanding Consumer Protection Risks Faced by Kenyan Digital Finance Users* (Innovations for Poverty Action, July 2020) https://poverty-action.org/study/understanding-consumer-protection-risks-faced-kenyan-digital-finance-users accessed on 20th February 2025.

conditions they are accepting.[227] This hurried approach to consent undermines the very essence of informed decision-making, allowing organisations to exploit a lack of understanding and awareness about what users are agreeing to.

In summary, the challenges posed by consent fatigue highlight the need for a re-evaluation of how informed consent is presented and implemented, ensuring that individuals can genuinely engage with and comprehend their choices regarding personal data.[228] Furthermore, the speed at which data is collected and analysed by DCPs, often in real-time, complicates the notion of consent as an ongoing process. Once consent is given, consumers seem to have little to no control over how their data is subsequently used or shared, particularly if they are unaware of their right to withdraw consent or the withdrawal processes are convoluted.[229] These pitfalls raise serious concerns about the effectiveness of the informed consent model in safeguarding consumer privacy in the digital credit ecosystem.

2.7 Impact of Frontier Technologies on Consumer Data Protection

The advent of frontier technologies[230] such as AI, blockchain, and the Internet of Things (IoT) have further complicated consumer data protection in DCS.[231] The advancements in these technologies have led to the development of more complex data collection and processing systems. These systems often function in a manner that is not transparent to consumers, as well as to those who manage the data. This lack of transparency has given rise to what are commonly referred to as black-box algorithms. These algorithms operate in a way that obscures their inner workings and decision-making processes, making it difficult to understand how inputs are transformed into outputs. As a result, users and data handlers may remain unaware of the underlying factors driving these automated systems, raising concerns about accountability, privacy, and potential biases in the data handling process.[232]

AI-driven credit scoring models can analyse a wide range of non-traditional data points, including factors such as social media interactions and online activities. By utilising advanced algorithms, these models create comprehensive profiles of individuals that extend beyond

---

227 Elizabeth Hildt *et al., Informed Consent in Digital Data Management*, (n 192) 14. Ivanfanta, *Do We Actually Agree to These Terms and Conditions?* (Data Science W231 | Behind the Data: Humans and Values, Ethical Legal Data Science, July 2021) https://blogs.ischool.berkeley.edu/w231/2021/07/09/do-we-actually-agree-to-these-terms-and-conditions/ accessed on 20th February 2025.

228 ibid (n 19) 35.

229 ibid (n 19) 35.

230 Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* (n 32)1880.

231 John Babikian, *Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era,* (n 142) 91.

232 ibid (n 135) 73.

conventional credit history and financial behaviours. This approach enables the collection of detailed insights into a consumer's habits, preferences, and social engagements.[233]

However, it is essential to consider that while these profiles may offer a more nuanced view of a person's financial potential, they do not always guarantee an accurate representation of the individual's creditworthiness.[234] Consequently, the reliance on such data can significantly influence a consumer's access to credit, potentially leading to decisions that may not fully reflect their financial reliability or capability. As the use of these models becomes more widespread, the implications for consumers, particularly those with limited traditional credit histories, raise important questions about fairness and privacy in the credit evaluation process.

In addition, the IoT allows for continuous data collection from devices embedded in consumers' daily lives, often without their explicit consent or awareness.[235] These developments necessitate rethinking and reconsidering traditional data protection models to account for the unique risks these technologies pose.

Emerging trends in data protection[236] include the rising importance of privacy-by-design, a proactive approach to embedding privacy measures into DCS's design and operation methods. This is in direct contrast with traditional reactive compliance methods, thus aligning with consumer-centric approaches that give users greater control over their personal data.

The use of blockchain technology to protect consumer data has become increasingly relevant in a rapidly digitising world.[237] Blockchain offers more secure and transparent systems for managing consent and data access by decentralising data storage and giving consumers control over their personal information.

2.8 Conceptualising Consumer Data Protection in Digital Credit Services in Kenya

Kenya's digital credit market has experienced significant growth, driven primarily by the rise of mobile money platforms and the widespread adoption of DCSs. These advancements have dramatically increased the accessibility and availability of digital financial services for a large segment of the population.[238] However, despite this progress, Kenya's consumer data protection remains relatively early. One of the most pressing issues is the pacing problem,

233 ibid (n 135) 73.
234 ibid (n 135) 73.
235 ibid (n 135) 83.
236 ibid (n 135) 75.
237 ibid (n 135) 83.
238 ibid (n 113) 1.

where the rapid expansion of digital credit services outstrips the development and enforcement of necessary regulatory frameworks to protect consumer data.[239]

The enactment of the DPA represented a pivotal milestone in Kenya's data privacy landscape. This legislation provides a legal foundation aimed at ensuring the effective protection of personal data and consumer rights. Notably, the DPA closely mirrors the European Union's GDPR, although it has been criticised for lacking some of the robust provisions found in the original framework.

Despite this important legal advancement, the implementation of the DPA faces considerable challenges. A significant portion of the consumer population is largely unaware of their rights regarding data protection under this legislation.[240] This lack of awareness is compounded by the inadequacies and inefficiencies in the oversight of DCPs, which raises concerns about the transparency and accountability of these entities in handling personal information.[241] As a result, the safeguards intended by the Act have not been fully realised, and many consumers remain vulnerable to potential misuse of their data.

A concerted effort is indispensable to effectively fortify the consumer data protection mechanisms within Kenya's rapidly evolving digital credit sector. This initiative should focus on raising awareness among consumers about their data rights, enhancing the enforcement of regulatory measures, and ensuring that the principles of informed consent are not only articulated but also implemented in a meaningful way.[242] By taking these steps, stakeholders can work toward creating a more secure and trustworthy environment for consumers engaging with digital financial services.

2.9 Conclusion

This chapter has explored the role of consent models and legislation in shaping consumer data protection in DCS. While models such as the informed consent model offer seemingly robust protections, they face challenges in ensuring proper and sufficient consumer awareness and

---

239 ibid (n 113) 8.

240 ibid (n 113) 8.

241 Mercy King'ori, *The Data Protection Act, 2019 as a Tool for Permitting Innovation and Consumer Safety in Kenya's Digital Finance Market*, (CIPIT, February 2020) https://cipit.strathmore.edu/the-data-protection-act-as-a-tool-for-permitting-innovation-and-consumer-safety-in-kenyas-digital-finance-market/ accessed on 21st February 2025.

242 Mercy King'ori, *The Data Protection Act, 2019 as a Tool for Permitting Innovation and Consumer Safety in Kenya's Digital Finance Market*, (CIPIT, February 2020) https://cipit.strathmore.edu/the-data-protection-act-as-a-tool-for-permitting-innovation-and-consumer-safety-in-kenyas-digital-finance-market/ accessed on 21st February 2025.

understanding. Legislation such as the DPA have introduced much-needed safeguards, but further refinement is necessary to address emerging trends and technological developments. As DCS continues to evolve, ongoing attention to consumer data protection will be critical to maintaining trust and security in the industry. Most importantly, the centrality of the legal and regulatory framework remains unquestionable. An analysis of this framework as is applicable in Kenya is pursued in Chapter Three of this thesis.

CHAPTER THREE
REGULATORY FRAMEWORKS GOVERNING CONSUMER DATA PROTECTION IN DIGITAL CREDIT SERVICES

3.1 Introduction

The preceding chapters have illustrated how DCSs have revolutionised financial inclusion in Kenya by providing swift and accessible credit to frequently unbanked and underserved populations. However, the increased reliance on personal data for credit assessment and lending decisions raises significant concerns regarding consumer protection, particularly in terms of consumer data privacy. The legal and regulatory frameworks governing consumer data protection within DCS are crucial for ensuring that service providers comply with legal standards and respect consumer rights. The rise of mobile and digital lending services in Kenya has led to the development of various legislative measures aimed at safeguarding consumer data within the digital credit market. This chapter seeks to explore these frameworks, with a particular focus on the incorporation of the informed consent model. Additionally, it will assess whether the current legislative framework sufficiently protects consumer data in the rapidly evolving landscape of digital credit.

3.2 Situating the Informed Consent Model in the Legal and Regulatory Frameworks

Informed consent is widely regarded as a fundamental principle of data protection, as it guarantees that consumers are fully aware of and agree to the ways in which their personal data is collected, used, and shared.[243] This principle is particularly vital in the context of DCSs, where extensive amounts of consumer data are regularly collected, processed, and shared across various digital platforms. Consumers in DCSs often provide personal information, including financial history, credit scores, and identification details, which are crucial for evaluating creditworthiness and determining loan eligibility.[244] It is essential for organisations in this field to not only inform their customers about the specific data being collected and the purposes for which it will be used but also to obtain explicit consent prior to processing any data. Furthermore, transparency regarding the sharing of this information with third parties - such as credit bureaus, financial institutions, or marketing agencies - is paramount. Consumers should have the right to understand how their data will be used, who will have access to it, and

[243] Omar Tene *et al., Big Data for All: Privacy and User Control in the Age of Analytics,* (n 129) 239.
[244] European Data Protection Supervisor, *Opinion 11/2021 on the proposal for a Directive on Consumer Credits,* (August 2021), 6.

the duration for which it will be retained.[245] By ensuring informed consent, companies can build trust with their customers, enhance their reputation, and comply with data protection regulations that safeguard consumer privacy in the digital age.

The legal framework governing consumer data protection in Kenya, particularly embedding the informed consent model, is incorporated within various statutes and regulations, including the Constitution of Kenya, 2010, the Competition Act, 2010, the Consumer Protection Act (CPA),[246] the DPA,[247] the Central Bank of Kenya Act (CBK Act),[248] and the CBK (DCP) Regulations.[249] Although it may appear straightforward to think of the informed consent model as an independent theory, each of these regulations is crucial in defining how informed consent is implemented within the digital credit landscape.

3.2.1 The Constitution of Kenya, 2010

The Constitution of Kenya establishes a robust framework dedicated to protecting personal data, placing significant emphasis on individuals' rights to maintain their privacy.[250] In particular, Article 31 of the Constitution explicitly enshrines the right to privacy for every citizen. This principle is foundational in safeguarding personal information as society increasingly relies on digital technology. This constitutional guarantee reinforces the importance of personal privacy and acts as a bulwark against invasive practices.

This right to privacy encompasses several vital aspects, including explicit protection against the unnecessary collection, use, or disclosure of personal data.[251] It asserts that individuals should maintain control over their personal information; thus, they should not be obliged to disclose it unless necessary. As technological advancements continue to evolve, thereby challenging the existing models - especially with the burgeoning of data-driven innovations - the imperative for comprehensive legislative measures to uphold this essential constitutional right becomes ever more crucial.[252] The dynamic nature of privacy rights necessitates that the

---

245 European Data Protection Supervisor, *Opinion 11/2021 on the proposal for a Directive on Consumer Credits,* (n 242) 10.
246 Cap. 504.
247 Cap. 411C.
248 Cap. 491.
249 Legal Notice 46 of 2022.
250 Constitution of Kenya, Article 31.
251 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17)
252 Ministry of Information, Communication and the Digital Economy, *Report of the Information, Communication and the Digital Economy Sectoral Working Group (SWG),* (June 2024), 107.

state adapts its legal frameworks and responsibilities to provide effective, meaningful protections for personal data.

At its core, the right to privacy is universally recognised as a fundamental human right. This acknowledgement is mirrored in key international instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), which collectively reinforce the legal foundation for privacy rights in Kenya.[253] These documents assert that every individual is entitled to maintain a private sphere - an area characterised by self-governance, personal interactions, and freedom - shielded from unnecessary or undue interference by governmental authorities or private organisations.[254]

Moreover, Kenya's status as a signatory to various international human rights treaties underlines the relevance of these global legal standards for its citizens. This relationship ensures privacy rights principles apply to individuals and organisations, including DCPs. This international context enriches and strengthens the constitutional protections surrounding personal data in the country.

The Kenyan judiciary has also played a pivotal role in articulating the right to privacy through landmark rulings. A notable case is *Kenya Legal and Ethical Network on HIV and AIDS (KELIN) and 3 Others v. Cabinet Secretary Ministry of Health and 4 Others*,[255] where the court sought to clarify the dimensions of privacy protection. In its ruling, the judiciary emphasised that the right to privacy serves as a safeguard against the unnecessary disclosure of sensitive personal information, particularly regarding individuals' family matters or private lives.[256] The court recognised that breaches of such confidentiality could lead to significant emotional distress and mental anguish, thereby underscoring the importance of protecting such information.

In this context, the right to privacy empowers individuals by reinforcing their autonomy and establishes clear boundaries concerning the collection, use, and dissemination of private information. Ultimately, it affirms an individual's entitlement to navigate life with minimal

[253] Article 12, Universal Declaration of Human Rights See also; Article 14, United Nations Convention on Migrant Workers. Article 17, International Covenant on Civil and Political Rights. Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms; and the Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality

[254] Martin Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, (A/HRC/17/34, 2009).

[255] (2016) eKLR.

[256] Mzalendo Trust, *Digital Rights in Kenya Report,* (2019), 8.

intrusion from external parties into their private affairs, reflecting a deep commitment to personal dignity and respect in an increasingly interconnected world.

3.2.2 The Consumer Protection Act, 2012

The Consumer Protection Act aims to rigorously protect the rights of consumers, particularly those who use DCPs' services.[257] Its main aim is to foster a climate of trust, allowing consumers to engage with these service providers with the assurance that their rights are recognised and safeguarded. To accomplish this objective, the Act imposes a series of clear and definitive obligations on service providers, ensuring that transparency and fairness are at the forefront of their interactions with consumers. For example, Section 16 of the Consumer Protection Act lays down a crucial stipulation: any agreement entered by a consumer can be nullified if established during a period marked by unfair practices. This provision is designed to empower consumers by enabling them to reclaim any losses or damages they might have incurred, thus demonstrating the legal system's firm commitment to promoting transparency and protecting consumer interests. Additionally, the Consumer Protection Act establishes robust protections concerning the handling of personal data. It mandates that service providers secure informed consent from consumers before collecting or sharing data. This requirement reinforces the necessity for service providers to clearly communicate comprehensive and precise information about their data-handling practices, thereby enshrining the principle of informed consent at the heart of these interactions. Moreover, the Consumer Protection Act allows consumers to seek legal redress when their rights have been violated.[258] It actively works against the profit-driven strategies often adopted by DCPs, particularly when these strategies conflict with borrowers' best interests.[259]

Despite permitting consumers the option to rescind agreements in response to identified unfair practices,[260] Significant challenges persist in the realm of digital credit. A primary hurdle is the information asymmetry that characterises the borrowing and lending processes. DCPs often rely on complex, opaque algorithms - referred to as 'black box' systems - to assess borrowers' creditworthiness, all too often without any human oversight or explicit consent from the

257 Consumer Protection Act 2019, s 3.
258 Consumer Protection Act 2019, Part IX.
259 International Financial Consumer Protection Organisation, "Review of Supervisory Tools for Suitable Consumer Lending Practices," (FinCoNet Report on Responsible Lending 2014) -<http://www.finconet.org/FinCoNetResponsible-Lending-2014.pdf >- accessed on 11th October 2024.
260 Consumer Protection Act 2019, s 16 (1).

borrowers themselves. This situation exemplifies a critical flaw in the informed consent model that the Consumer Protection Act aims to uphold.

The right to rescind, as outlined in the Consumer Protection Act, is intended to revert both parties to their original states prior to the contract.[261] However, in the context of digital credit, achieving this restoration proves to be a practical impossibility. Once a consumer engages with a DCP, the provider typically amasses extensive amounts of personal data, resulting in a stark information imbalance. The DCP possesses significantly more information about the borrower than the borrower has about the provider, placing the consumer in a precarious position.

In addition, credit agreements may not always be formalised in writing; they can also exist in verbal or implied forms. Nevertheless, the Consumer Protection Act mandates that all credit agreements be documented in written form.[262] This requirement is essential as it ensures that consumers fully understand the terms and conditions they accept before participating in a credit transaction. Furthermore, the Consumer Protection Act defines an 'unfair event' sufficiently broadly to include incidents occurring prior to and after signing an agreement. By dint of this provision, a pertinent example of an unfair event might be the application of ML algorithms that evaluate a borrower's profile, potentially subjecting them to less advantageous loan terms or higher interest rates than other consumers.[263] Often, such unfavourable terms may not be clearly articulated in the initially agreed-upon conditions. Borrowers may, therefore, struggle to grasp the implications of these terms, further exposing them to vulnerabilities within the informed consent framework that the Act seeks to establish.

In summation, while the Consumer Protection Act aims to bolster consumer protection in the digital credit ecosystem, various procedural and systemic challenges arise that impede its effective implementation. These challenges are especially pronounced due to the existing information disparities and the often-opaque nature of algorithmic decision-making processes.

3.2.3 The Competition Act, 2010

The rapid rise of digital credit in Kenya has transformed financial accessibility, enabling millions of unbanked Kenyans to obtain loans at the comfort of their mobile phone. However, with this rapid growth, consumers have been exposed to unethical lending practices ranging from hidden fees to exploitative interest rates, aggressive debt collection tactics and even biases

261 Consumer Protection Act 2019, s 16.
262 Consumer Protection Act 2019, s 34.
263 Stefan Larsson, *Algorithmic Governance and the Need for Consumer Empowerment in Data-Driven Markets,* (Internet Policy Review, Vol. 7, Issue 2, May 2018), 4.

algorithms. Section 56(2)(c) and Section 57(2)(c) of the Competition Act serve as critical safeguards against such conduct, ensuring fair competition and protecting consumers from exploitation.

Section 56 (2) (c) prohibits businesses from engaging in behaviour that may be termed as being unconscionable conduct when dealing with consumers.[264] Unconscionable conduct has been defined as behaviour that is excessively unfair, deceptive or exploitative often taking advantage of a consumer's lack of understanding, bargaining power or urgency. In the context of digital credit, this includes lenders who misrepresent loan terms, charge excessive interest and even used biased algorithms to determine consumer interest rates. The enforcement of this provision allows the Competition Authority of Kenya (CAK) to investigate unfair lending practices and take corrective measures such as imposing fines and even working together with the CBK in revoking licences of DCPs.

Section 57 (2) (c)[265] while complementing Section 56, reinforces consumer protection through the prohibition of suppliers from accepting payments for goods or services they have no intention of supplying as agreed. In the digital credit space, lenders are monitored to ensure that they provide the agreed upon loan amounts and the conditions promised at the time of borrowing. Instances where the biased algorithm alters the interest rate of a particular borrower or its use without informing the borrower would be classified as unconscionable conduct.

---

[264] Section 56(2)(c) of the DPA states as follows: "…*Without limiting the matters to which the Authority may have regard for the purpose of determining whether a person has contravened subsection (1) in connection with the supply or possible supply of goods or services to another person (in this subsection referred to as "the consumer"), the Authority may have regard to—(a)the relative strengths of the bargaining positions of the person and the consumer;(b)whether, as a result of conduct engaged in by the person, the consumer was required to comply with conditions that were not reasonably necessary for the protection of the legitimate interests of the person;(c)whether the consumer was able to understand any documents relating to the supply or possible supply of the goods or services;(d)whether any undue influence or pressure was exerted on, or any unfair tactics were used against, the consumer or a person acting on behalf of the consumer by the person acting on behalf of the person in relation to the supply or possible supply of the goods or services; and(e)the amount for which, and the circumstances under which, the consumer could have acquired identical or equivalent goods or services from another supplier…*"

[265] Section 57(2)(c) of the DPA states as follows "…*Without limiting the matters to which the Authority may have regard for the purpose of determining whether a person, being a supplier, has contravened subsection (1) in connection with the supply or possible supply of goods or services to a business consumer, the Authority may have regard to—(a)the relative strengths of the bargaining positions of the supplier and the business consumer;(b)whether, as a result of conduct engaged in by the supplier, the business consumer was required to comply with conditions which were not reasonably necessary for the protection of the legitimate interests of the supplier;(c)whether the business consumer was able to understand any documents relating to the supply or possible supply of the goods or services*…"

3.2.4 The Central Bank of Kenya Legal and Regulatory Framework

The CBK Act plays a vital yet indirect role in overseeing and regulating DCSs within Kenya's financial landscape. While the CBK Act does not explicitly emphasise data protection, it sets up a comprehensive regulatory framework that governs financial institutions, including DCPs, under the vigilant supervision of the CBK.[266] The CBK's primary responsibility is to ensure that financial institutions operate with utmost integrity and transparency, thereby building public confidence in the financial system. This responsibility extends to consumer protection as a key component of its supervisory duties.[267] In this regard, the CBK is tasked with enforcing compliance with existing data protection laws and ensuring that DCPs align their operations with principles of informed consent when handling consumers' personal information.

The CBK's supervisory role is crucial, granting it the authority to impose sanctions on DCPs that fail to comply with relevant data protection regulations. This enforcement mechanism is essential to upholding the informed consent model, which requires that consumers be adequately informed about how their personal data is collected, used, and stored. However, it is important to recognise that the CBK's overarching mandate of ensuring the "safety and soundness" of banks and lenders may not always align with a comprehensive approach to consumer protection.[268]

One significant limitation of the framework established by the CBK Act is that consumers rely on the actions of third parties, such as regulatory bodies like the CBK, to safeguard their rights.[269] This creates a scenario where individual borrowers may feel vulnerable and powerless, lacking a direct path to advocate for their own interests. As a result, consumers might find themselves waiting for the CBK to act, leading to potential delays in addressing their rights violations.

Advocating for an amendment to the Act that empowers individuals to submit complaints directly to the CBK could represent a significant step toward enhancing consumer protection. Such reforms would allow for quicker response times and ensure that individual grievances are addressed promptly. Nevertheless, the success of this proposal depends on the integrity and effectiveness of the CBK. If the Central Bank operates in a compromised state or becomes

---

266 Central Bank of Kenya Act 2023, s 4A.
267 Central Bank of Kenya Act 2023, s33R.
268 Central Bank of Kenya Act 2023, s 4.
269 John Kamau, *How National Bank Was Brought To Its Deathbed* (September 2019) https://nation.africa/kenya/news/politics/how-national-bank-was-brought-to-its-deathbed-203802 accessed on 21st February 2025.

susceptible to corruption, it could undermine the implementation and enforcement of essential consumer protections, ultimately failing to safeguard borrowers' interests adequately. This is as evidenced by the National Bank of Kenya (NBK) that was faced with significant challenges due to the non-intervention of the CBK and an extreme failure of consumer protection. The fiasco involving the NBK was that it provided unsecured loans to borrowers who seemingly had no intention to repay the borrowed amounts. The CBK failed to intervene in the collapsing bank, and the National Social Security Fund (NSSF) intervened in bailing out the bank, however, it was part of the problem. The NSSF used depositor money in an attempt to rescue the bank, even going so far as converting the debt to equity, however, this still failed and the bank collapsed.[270]

In 2022, the CBK made a significant advancement by introducing the CBK (DCP) Regulations, which were designed to establish a comprehensive regulatory framework for digital lenders operating in Kenya. The Central Bank of Kenya (Amendment) Act, 2021, which introduced the phenomenon of DCP regulation in central banking terms - preceded DCP Regulations. This initiative encompassed well-known companies in the digital lending space, such as Branch and Tala, which have gained popularity for their accessible credit services. The regulations borrowed significantly from the DPA and other applicable privacy laws, mandating that digital lenders uphold stringent compliance standards aimed at safeguarding consumer information.[271] One critical component of these regulations is the requirement that digital lenders secure explicit and informed consent from borrowers before they can collect or process any personal data.[272]

This stipulation is pivotal as it enhances the informed consent model within the digital lending sector, ensuring that individuals who seek DCSs are genuinely aware of their rights concerning data privacy. Consumers must be fully informed about what personal information is being gathered, how it will be utilised, and the potential implications of sharing their data with these financial institutions. By reinforcing these regulations, the CBK aims to promote transparency, protect consumers from data misuse, and contribute to a more secure digital financial environment in Kenya.

[270] John Kamau, *How National Bank Was Brought To Its Deathbed* (n 267).
[271] The Central Bank of Kenya (Digital Credit Providers) Regulations 2021, s 4.
[272] The Central Bank of Kenya (Digital Credit Providers) Regulations 2021, s 26.

3.2.5 The Data Protection Act, 2019

The cornerstone of data privacy and protection legislation in Kenya is the DPA, a comprehensive statute that operationalises Article 31 of the Kenyan Constitution, which enshrines the right to privacy.[273] The DPA intricately outlines a set of principles that guide the processing of personal data, ensuring that data controllers and processors, including DCPs, adhere to a framework designed to safeguard individual rights. A central aspect of this legal structure is the requirement for DCPs to obtain informed consent from data subjects before collecting or using their personal information. This consent must be specific, voluntarily given, and well-informed, ensuring that individuals fully grasp their agreement's implications before any data processing takes place.[274] The DPA establishes the ODPC, an authoritative body responsible for overseeing the implementation of the Act's provisions, to bolster compliance and governance within this framework.[275] The ODPC's mandate encompasses monitoring the adherence of various entities - including government agencies, private organisations, and other bodies that handle personal data - to the DPA's standards. This office not only guides DCPs in their operations but also plays a crucial role in protecting consumers' rights regarding their personal data.

The DPA has significant implications for the DCS landscape in Kenya, notably the explicit and informed consent requirement placed on DCPs.[276] This essential stipulation seeks to empower consumers, especially those in vulnerable positions, such as borrowers, by ensuring they are fully aware of the purposes for which their data is collected and used. For instance, if a DCS plans to analyse a consumer's mobile phone metadata to assess their creditworthiness, it is imperative that the service provides clear and transparent disclosure about this intent. Additionally, consumers must feel free to provide their consent, without any pressure or coercion. However, a notable challenge arises as many individuals may find it difficult to fully comprehend the ramifications of granting such consent.

Another fundamental tenet of the DPA is the principle of data minimisation, which stipulates that personal data should only be retained for a specified and necessary duration.[277] Once this

---

[273] Article 31 of the Constitution of Kenya 2010 states thus: *"Every person has the right to privacy, which includes the right not to have—(a)their person, home or property searched;(b)their possessions seized;(c)information relating to their family or private affairs unnecessarily required or revealed; or(d)the privacy of their communications infringed."*

[274] Data Protection Act 2019, s 25. See also Data Protection Act 2019, s 26.

[275] Data Protection Act 2019, s 5.

[276] Data Protection Act 2019, s 26.

[277] Data Protection Act 2019, s 25.

period expires or the data is no longer required for its intended purpose, it must be securely disposed of. This directive aims to mitigate the risks associated with the indefinite retention of data, thereby reducing potential vulnerabilities to misuse or unauthorised access. DCPs are also mandated to implement robust technical and organisational safeguards to protect personal data from breaches and unauthorised access, thereby enhancing the overall security of consumer information.[278]

The ODPC is responsible for enforcing the DPA's provisions and registering DCPs as recognised data controllers or processors.[279] This registration process is accompanied by regular audits to verify compliance with the DPA's stipulations and to levy penalties in cases of non-compliance. Additionally, the ODPC serves as a critical resource for consumers, handling grievances from individuals who believe their data rights have been violated.[280] For example, if a consumer suspects that his or her personal information has been utilised without proper authorisation, they have the right to lodge a complaint with the ODPC. The ODPC has the authority to investigate these claims and implement corrective actions, including fines on errant entities.

Notably, one of the distinguishing features of the DPA is its extraterritorial reach. It mandates that even DCPs operating outside of Kenya must comply with the Act's provisions when handling the personal data of Kenyan citizens. This aspect is particularly significant in an era where data collection services frequently intersect with global partnerships, particularly those involving fintech companies or foreign investors. The extraterritorial scope of the DPA introduces intricate challenges related to enforcing jurisdictional data rights and the registration requirements for cross-border DCPs. Moreover, the inherent risks associated with cross-border data transfers further complicate ensuring effective consumer data protection.

In the landmark case of *The Coalition for Reform and Democracy (CORD) and 2 Others v. Republic of Kenya and 10 Others*,[281] the Kenyan judiciary articulated a crucial legal doctrine by asserting that the right to privacy is not an absolute right. Instead, the court emphasised the necessity of conducting a balancing act, weighing any intrusions into an individual's privacy against the public interest that may be served by such actions. This ruling highlights the

[278] Data Protection Act 2019, s 41.
[279] Data Protection Act 2019, s 18.
[280] Data Protection Act 2019, s 9.
[281] [2015] eKLR.

complex interplay and evolving nature of privacy rights, particularly as they relate to legitimate governmental and societal interests.

Similarly, in the case of *Musa Wesutsa v Azura Credit Limited T/A Truepesa,*[282] the Complainant filed a complaint with the ODPC alleging that he had been receiving phone calls and emails regarding a loan he did not apply for. The ODPC in its investigations found that the Respondent, by not informing the Complainant of the use to which his personal data was to be put at the point of collection of the personal data, violated his right to be informed. Furthermore, the Respondent collected the emails from a third party and failed to inform the Complainant that his email was being collected for the purpose of being listed as referee/emergency contact to its customer and failed to give the Complainant an opportunity to consent to the listing. The Respondent was found liable in this matter.

3.3 Analysing Scenarios for the Informed Consent Model's Adequacy in Law

The informed consent model serves as a vital element within Kenya's legal and regulatory framework for data protection, playing a significant role in safeguarding individuals' privacy and autonomy over their personal information. However, the effectiveness of this model is not uniform; it largely depends on the way it is put into practice. In this section, we will delve into two illustrative scenarios that will help evaluate the advantages and disadvantages of the informed consent model as it currently operates within the legal landscape. These examples will highlight the varying outcomes that can arise from different implementation strategies and underscore the importance of context in shaping the efficacy of informed consent for data protection in Kenya.

3.3.1 Scenario 1: The Model Works Optimally (Strengths Overshadow the Flaws)

In this scenario, the informed consent model operates effectively, ensuring that DCPs adhere meticulously to established legal standards and regulations governing the handling of personal data. Consumers are provided with comprehensive and clear information that details how their personal data will be utilised, stored, and shared. This information is transparent and designed to empower consumers by enabling them to make informed choices regarding their personal information. Consumers are given the opportunity to grant informed, specific, and unequivocal

[282] ODPC Complaint No. 1088 of 2024.

consent, which is critical in distinguishing legitimate data practices from those that might infringe on personal privacy.[283]

The optimal consent process is designed to be comprehensive, encompassing all aspects of data usage, thus ensuring that consumers understand exactly what they are agreeing to. Furthermore, the regulatory oversight provided under the DCP Regulations plays a pivotal role in maintaining the integrity of this model. This oversight ensures that any potential breaches of data privacy are swiftly identified and addressed. In the event of a data breach or violation of consent, consumers have recourse to a variety of remedies. These remedies may include monetary penalties imposed on the offending company by the ODPC, reinforcing the seriousness of compliance with data protection laws. The effectiveness of this informed consent model lies in its core principles of transparency, consumer empowerment, and the accountability of DCPs. By implementing these principles effectively, the framework protects consumer rights and fosters a sense of trust between consumers and DCPs. This trust is essential for encouraging broader acceptance and adoption of DCSs. Ultimately, when consumers feel confident that their data is handled responsibly and ethically, it paves the way for a more collaborative relationship between consumers and data controllers, benefiting both parties in an increasingly data-driven world.[284]

3.3.2 Scenario 2: If The Model Does Not Work Optimally (Flaws Overshadow the Strengths)

In this second scenario, the informed consent model reveals considerable limitations that significantly undermine its intended benefits. These shortcomings often become evident when DCPs fail to give consumers adequate information for making informed decisions. For instance, consent may be acquired through misleading practices, such as bundling consent for data collection with other unrelated services, which can obscure consumers' understanding of what they are agreeing to. Additionally, the use of complex legal jargon and technical language in consent forms can create further barriers, making it exceedingly difficult for the average consumer to fully grasp the implications of their consent. Moreover, the enforcement of

[283] Office of the Data Protection Commissioner, *Guidance Note for the Communication Sector,* (December 2023), 15.

[284] Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller, *The Consumer-Data opportunity and the Privacy Imperative,* (McKinsey and Company, April 2020) https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative accessed on 19th February 2025 See also; Timothy Morey, Theodore Forbath and Allison Schoop, *Customer Data: Designing for Transparency and Trust* (Harvard Business Review, Analytics and Data Science, May 2015) https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust accessed on 21st February 2025.

existing data protection laws is frequently inadequate due in part to limited regulatory resources and insufficiently informed consumers who may not be aware of their rights regarding personal data. This environment fosters a situation where the informed consent model does not effectively protect consumer interests. Consequently, this leads to the misuse of personal data, manifesting in various forms such as unauthorised sharing with third parties, excessive and unnecessary data collection practices, and a pervasive lack of transparency regarding how data is handled.[285] These identified weaknesses not only highlight the limitations of the informed consent model in its current form but also emphasise the urgent need for more robust enforcement mechanisms that can address these issues. There is a pressing call for increased public awareness initiatives that educate consumers about their rights and the implications of their consent. Alongside this, ongoing reviews and updates to the legal framework governing data collection and sharing practices are essential to effectively tackle the evolving challenges present in this rapidly changing digital landscape. Such measures are crucial to ensure that consumer data is safeguarded and that individuals can exercise genuine control over their personal information.[286]

3.4 Situating the Impact of Frontier Technologies on the Model and Regulation

The rise of frontier technologies - including AI, ML, big data analytics, and blockchain - has significantly reshaped the landscape of digital credit. These cutting-edge innovations offer transformative approaches to evaluating creditworthiness, enabling lenders to utilise vast amounts of data to make assessments of an individual's or business's financial reliability. By leveraging machine learning algorithms, for example, financial institutions can identify patterns and trends that were previously undetectable, leading to more tailored credit offerings that suit the unique needs of each customer.

Furthermore, these technologies enhance operational efficiency across the financial sector. Automated systems reduce the time and resources required for loan approvals and credit assessments, streamlining processes that were once labour-intensive. This speed and efficiency allow for a more responsive lending environment, where consumers can access credit more quickly and easily.

However, despite these advancements, integrating such technologies is not without its challenges. The complexities inherent in the algorithms used for credit assessments pose

[285] ibid (n 261) 2.
[286] ibid (n 261), 2.

significant questions about transparency and accountability. Traditional models of informed consent, which rely on individuals fully understanding the terms and implications of their agreements, may not be effective in this new landscape. Many users may not realise how their data is being collected, analysed, and utilised, raising ethical concerns about privacy and consent.

Additionally, the regulatory frameworks that currently govern credit practices are often ill-equipped to address the rapidly evolving nature of these technologies. As innovations outpace existing regulations, there is a pressing need for new policies that ensure consumer protection while fostering technological growth. Balancing innovation with regulatory oversight is critical to maintaining trust in the digital credit system, and it requires collaboration among stakeholders, including regulatory bodies, financial institutions, and consumers themselves. In the end, it can be argued that the implications of frontier technologies can easily lead to transition from the first scenario to the second scenario or at least render attainment of the first scenario challenging that putting into test the adequacy of the informed consent model in consumer data protection in DCSs. Some of the salient fronter technologies are highlighted hereinafter in turns.

3.4.1 Artificial Intelligence and Machine Learning in Digital Credit Services

This section explores the dual impact of AI and ML in DCS, focusing on their functionality, benefits, and risks. AI and ML have emerged as transformative forces within DCSs, empowering DCPs to streamline credit assessments, automate decision-making processes, and deliver customised financial solutions.[287] These technologies leverage extensive datasets to predict creditworthiness, evaluate risks, and optimise lending practices, all while providing faster, more efficient, and more accessible credit products.[288]

However, alongside the opportunities for innovation and enhanced financial inclusion, significant challenges arise regarding consumer data protection and the effectiveness of the informed consent model. These systems often function as 'black boxes,' where decision-making processes remain incomprehensible even to their developers.[289] This lack of

[287] Tayyab Muhammad, Asad Yaseen, Kriya Shah, *Empowering Financial Services: The Transformative Impact of AI on FinTech Innovation,* (American Journal of Computing and Engineering, Vol. 7, Issue 4), 36.

[288] Amit Taneja, *The Transformative Impact of Artificial Intelligence in Financial Services: Enhancing Decision-Making, Efficiency, and Risk Management*, (International Research Journal of Engineering and Technology, Vol. 11, Issue 07, July 2024), 557.

[289] International Telecommunications Union (ITU), *Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective,* (n 26) 19.

transparency undermines the fundamental principles of informed consent, as consumers - particularly borrowers - are unable to fully grasp how their data is being used and the associated implications. For instance, AI systems can analyse unconventional datasets such as social media activity or geolocation data, which could lead to biased or unfair credit decisions. In the absence of algorithmic accountability, the fairness and legality of these decisions cannot be validated, potentially violating consumers' rights to informed and voluntary consent as mandated by the DPA. Regulators must, therefore, promote AI transparency, ensuring that providers disclose how algorithms utilise consumer data and implement safeguards against discriminatory practices. It is on account of the foregoing background that this section delves into AI and ML's dual impact on DCSs, focusing on their roles, benefits as well as associated risks.

3.4.1.1 The Role of AI and ML in DCS

AI and ML play a critical role in analysing large datasets, facilitating the identification of intricate patterns, predicting future trends, and automating various tasks, particularly those characterised by repetition. In the context of DCS, these technologies support multiple functions, especially in the domain of credit scoring. AI-driven credit scoring models leverage diverse data sources that extend beyond conventional financial metrics.[290] These sources encompass mobile phone usage patterns, payment histories, geolocation data, and social media behaviours. By integrating these varied data points, such models provide a comprehensive assessment of an individual's creditworthiness, resulting in more accurate and inclusive credit evaluations.[291] One of the primary advantages of contemporary credit scoring systems is their ability to incorporate nontraditional data, which is particularly beneficial for unbanked populations - an extensive demographic in Kenya.[292] By moving away from traditional credit metrics such as formal employment or established banking relationships, AI-enhanced methodologies promote broader access to credit for individuals who may have previously been considered uncreditworthy. This transformation supports financial inclusion.

---

290 Tayyab Muhammad *et al.*, *Empowering Financial Services: The Transformative Impact of AI on FinTech Innovation,* (n 284) 40. See also; Hariharan Pappil Kothandapani, *Leveraging AI for Credit Scoring and Financial Inclusion in Emerging Markets*, (World Journal of Advanced Research and Reviews, Vol. 12, Issues 03, 2022), 526.

291 Wilhelmina Addy, Adeola Ajayi-Nifise, Binaebi Bello, Olubusola Odeyemi, Titilola Falaiye, *AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analysis*, (Global Journal of Engineering and Technology Advances, February 2024), 119.

292 Kaushikkumar Patel, *Credit Card Analytics: A review of Fraud Detection and Risk Assessment Techniques*, (International Journal of Computer Trends and Technology, Vol. 71), 69.

Moreover, ML algorithms excel in predicting the likelihood of loan defaults by analysing borrower behaviour patterns. This functionality empowers DCPs to implement more effective risk mitigation strategies.[293] Enhanced accuracy in risk assessments enables DCPs to make informed lending decisions and optimise portfolio performance. Additionally, AI empowers DCPs to customise credit solutions tailored to the distinct profiles of individual borrowers. By considering specific preferences, financial behaviours, and individual circumstances, lenders can offer personalised lending options that align more closely with borrowers' needs.[294] This individualised approach enhances the customer experience, contributes to improved repayment rates, and fosters enduring relationships with clients, thereby supporting a more sustainable lending ecosystem.

3.4.1.2 Challenges to the Informed Consent Model in AI and ML Use

The integration of AI and ML within DCSs creates complex challenges that can significantly impact the traditional informed consent model, which has long been considered a cornerstone of data protection practices. While informed consent is designed to empower individuals by ensuring they understand how their data will be used, the characteristics inherent in AI and ML technologies pose specific obstacles to achieving true transparency.[295]

One of the primary challenges is the opacity in decision-making processes, often referred to as the 'black box effect.'[296] This phenomenon occurs when the algorithms that drive AI and ML systems operate in ways that are not easily understandable or interpretable by humans. As a result, individuals may find it difficult to comprehend how their data influences outcomes, making it nearly impossible to provide meaningful consent.

Additionally, the complexity of data processing in these systems compounds the challenge. AI and ML algorithms can analyse vast amounts of data from diverse sources, often involving intricate models that evolve over time. This complexity can obscure the pathways through which data is utilised, further complicating individuals' ability to grasp the implications of their consent.[297]

---

293 ibid (n 288), 121.
294 ibid (n 288), 121.
295 Amit Taneja, *The Transformative Impact of Artificial Intelligence in Financial Services: Enhancing Decision-Making, Efficiency, and Risk Management*, (n 285) 557. See also; Heike Felzmann, Eduard Fosch Villaronga, Christoph Lutz and Aurelia Tamo-Larrieux, *Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns,* (Big Data and Society, January – June 2019), 5.
296 ibid (n 26) 19.
297 ibid (n 26) 19.

Furthermore, there is the issue of potential biases that can be embedded within these algorithms. AI systems are often trained on historical data that may reflect existing societal biases, leading to outcomes that can perpetuate discrimination or unfair treatment. When users are asked to consent in such contexts, they may be unaware of these biases and the associated risks, undermining the foundational principles of informed consent. In summary, the application of AI and ML in DCSs introduces significant hurdles that jeopardise the integrity of the informed consent model, highlighting the need for enhanced transparency, ethical considerations, and user education to protect individuals' rights in the data-driven landscape.

3.4.1.2.1 Opacity of AI and ML systems (Black Box' Models)

AI systems, particularly those employing deep learning technologies and methodologies, are often characterised as 'black boxes.' This terminology arises from their inherent lack of transparency concerning the decision-making processes and rationale behind those decisions.[298] While these systems can achieve remarkable accuracy in generating predictions or classifications, their internal mechanics often remain obscure, not only to end users but also to the developers responsible for their design and implementation.[299] For instance, consider an AI model that evaluates loan applications to determine approval or denial. This model may utilise complex patterns derived from extensive datasets that encompass various borrower attributes, transaction histories, and credit scores. However, the underlying reasoning for the approval or denial of a specific application may not be readily apparent. Such ambiguity poses significant challenges for borrowers seeking to comprehend their financial standing and the determinants influencing the lender's judgment. Similarly, lenders may encounter difficulties in providing clear justifications for their decisions, leading to a lack of accountability.[300]

This scenario gives rise to critical concerns regarding informed consent, especially when analysed in the context of the DPA. The intrinsic opacity of these AI systems fundamentally undermines the principle of transparency, which is essential to the DPA.[301] When borrowers are requested to consent to the processing of their personal data by these systems, they may not fully understand how their information will be used or the potential implications of its use. As a result, this lack of clarity presents substantial obstacles for consumers attempting to provide

---

298 Addy Wilhelmina *et al., AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analysis*, (n 288), 122.

299 Bryce Goodman, and Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a Right to Explanation,* (AI Magazine, Association for the Advancement of Artificial Intelligence, 2017), 55.

300 ibid (n 26) 19.

301 ibid , (n 26) 19.

genuinely informed consent.[302] The DPA stipulates that consent must be specific, informed, and unequivocal; however, when the mechanisms of decision-making are enigmatic, it becomes increasingly challenging for individuals to grasp what they are consenting to, thereby jeopardising compliance with the DPA's requirements. This transparency deficit is an escalating concern in an age where data-driven decision-making is becoming ubiquitous, highlighting the necessity for a thorough examination of how to ensure the protection of consumer rights while harnessing the capabilities of advanced AI systems.[303]

3.4.1.2.2 Potential Bias and Discrimination

The principle of "Garbage In, Garbage Out" (GIGO) in computing emphasises that the effectiveness and accuracy of AI and machine learning systems are inextricably linked to the quality and integrity of the data utilised for their training.[304] When the training datasets are marred by inherent biases - especially those rooted in historical injustices like discriminatory lending practices - there is a significant risk that the AI models will not only replicate these biases but may also amplify them.[305] For example, credit scoring models built on biased datasets may systematically disadvantage low-income borrowers by excluding them from favourable lending terms, thus perpetuating a cycle of inequality in financial access.

In such scenarios, the framework of informed consent raises critical concerns. Consumers may unwittingly agree to the processing and analysis of their personal data without fully understanding the potential ramifications. As a result, they might consent to systems that have been trained in a way that leads to discriminatory outcomes, further entrenching existing disparities.[306] The repercussions of biased algorithms can disproportionately affect marginalised communities, posing a significant challenge to the concept of fairness enshrined in Kenya's legal and regulatory frameworks, which aim to protect all individuals from discrimination.[307]

Additionally, the presence of biased algorithms can pave the way for predatory lending practices by DCPs. These practices often manifest through elevated interest rates and

---

302 ibid , (n 26) 19.

303 ibid (n 26) 19.

304 Oksana Zdrok, *Why "Garbage In, Garbage Out" Should Be the New Mantra for AI Implementation*, (Shelf, May 2024) https://shelf.io/blog/garbage-in-garbage-out-ai-implementation/ accessed on 21st February 2025.

305 Addy Wilhelmina *et al., AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analysis*, (n 288), .

306 Bryce Goodman *et al., European Union regulations on algorithmic decision-making and a 'right to explanation*, (n 296) 53.

307 Faith Gordon, *Virginia Eubanks – Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, (New York: Picador, St Martin's Press, Law, Technology and Humans, Vol. 1(1), 2018), 163.

unfavourable loan conditions predominantly imposed on low-income borrowers, exacerbating their financial hardships. The design of biased algorithms may involve analysing and categorising data in a manner that fails to account for the complexities and challenges faced by individuals with limited access to resources.[308] This not only further marginalises these individuals but can also lead to systemic inequalities in access to credit and financial services, highlighting a pressing need for reform in data practices and algorithmic transparency to safeguard against discrimination.[309]

3.4.2 Big Data Analytics and Consent Complexity

The realm of big data analytics has dramatically reshaped the operations of DCPs, providing them with the capability to harness vast quantities of both structured and unstructured data. This transformative shift has paved the way for more precise credit scoring models and significantly enhanced fraud detection mechanisms, enabling DCPs to develop personalised financial services tailored to the unique needs of their customers. The capabilities unlocked by big data closely mirror those offered by AI and ML, allowing DCPs to move beyond traditional evaluation methods that rely heavily on a borrower's established financial history.[310] By performing in-depth analyses of trends and patterns derived from diverse data sources, DCPs can make well-informed lending decisions, fostering greater financial inclusion for historically unserved and underserved communities.[311] The ability to access a broad spectrum of data sets grants DCPs deeper insights into potential borrowers, significantly reducing the risks associated with defaults and improving overall loan performance.

However, integrating such advanced analytics comes with its own set of challenges, particularly regarding informed consent. Many consumers find themselves struggling to track or manage how their personal data is shared or utilised, leading to a landscape where data privacy is increasingly compromised. A common practice within AI systems, known as 'data fusion', entails aggregating information from multiple sources, including various third-party databases.[312] This synthesis can unveil insights that would remain elusive with analyses based solely on individual data sets. A worrying aspect of this scenario unfolds when consent provided for a specific service inadvertently allows for data sharing with numerous third

---

308 ibid (n 304)163.
309 ibid (n 304)163.
310 Solon Barocas, Moritz Hardt, and Arvind Narayanan, *Fairness and Machine Learning*, (The MIT Press December 2023).
311 Solon Barocas *et al*., *Fairness and Machine Learning* (n 307).
312 Federica Mandreoli, Manuela Montangero, *Data Handling in Science and Technology,* (Chapter 9, Data handling in Science and Technology, 2019).

parties.[313] This situation not only amplifies the risks of data misuse but also fosters a lack of transparency, placing consumers in a precarious position regarding their personal information. Alarmingly, a legislative void permits DCPs to utilise publicly accessible data without stringent oversight. This raises essential questions around data rights wherein concerns arise if a third party collects information and subsequently makes it publicly available, putting into issue whether the rights of the original data subjects remain intact in such cases.[314]

This intricate and often opaque data-sharing ecosystem raises significant concerns about the specificity and clarity of consent requirements established by current data protection laws. As a potential solution, regulators might consider the need for more explicit, service-specific consent forms to ensure that consumers are adequately informed. Furthermore, DCPs could be required to obtain fresh, informed consent for any data-sharing initiatives extending beyond the original agreement's bounds.

Big data analytics empowers DCPs to reimagine traditional credit assessment methodologies, which have historically been anchored in established financial histories such as credit reference bureau listings. In contrast, contemporary systems analyse a broad spectrum of data points, including mobile phone metadata. This category encompasses an individual's call logs, SMS exchanges, and mobile money transactions[315] - such as those conducted through platforms like MPesa and Airtel Money. Such data can provide invaluable insights into an individual's financial behaviour and spending patterns, though it is crucial to note that this information might not always convey a complete picture of a person's overall financial stability.

Additionally, social media activity plays a critical role within this analytical framework. While social media data is often viewed as publicly accessible, AI algorithms can delve into a user's interactions to draw conclusions about their creditworthiness. Factors considered may include the stability and characteristics of an individual's social network, their communication patterns, and even travel history as depicted in their online profiles.[316]

---

313 Elizabeth Kivuva, *Kenyan Firms on the Spot for Sharing Customer Data,* (Business Daily, July 2021) *Kenyan firms on the spot for sharing customer data - Business Daily* accessed on 19th February 2025. See also; Grace Mutung'u, Third Party Data Sharing: Analysis of the Data Protection Bill, 2019, (CIPIT, October 2019) https://cipit.strathmore.edu/third-party-data-sharing-analysis-of-the-data-protection-bill-2019/ accessed on 19th February 2025.

314 Elizabeth Kivuva, *Kenyan Firms on the Spot for Sharing Customer Data,* (n 310) See also; Grace Mutung'u, Third Party Data Sharing: Analysis of the Data Protection Bill, 2019 (n 310).

315 Michelle Kaffenberge, Edoardo Totolo, and Mattew Soursourian, *A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania*, (CGAP, October 2018), 4.

316 Zirui Shao, *Big Data Revolution in Finance: Opportunities, Challenges, and Future Trends* (Proceedings of the 2nd International Conference on Management Research and Economic Development), 73.

Moreover, geolocation data serves as another vital element that can be leveraged to assess a borrower's stability, particularly within rural or mobile populations. By estimating an individual's location and evaluating their environment's socioeconomic conditions and prevailing borrowing trends, DCPs can potentially achieve a more nuanced understanding of a consumer's creditworthiness.

The comprehensive collection and synthesis of such multifaceted data can also aid in establishing a borrower's purchasing history and tracking their e-commerce transactions. This information is invaluable for DCPs, enabling them to conduct a more refined assessment of repayment capabilities and spending behaviours, ultimately enhancing their lending practices.[317] These innovative, data-driven insights present promising opportunities for lenders and borrowers in a landscape where traditional credit histories may be insufficient.

3.4.3 Blockchain Technology and Consent Challenges

Blockchain has emerged as a powerful tool for enhancing transparency, security, and efficiency in DCS. With its decentralised and immutable architecture, blockchain is increasingly being used for secure data storage and transactions in DCS.[318] While its security benefits are evident, it presents unique challenges for the informed consent model.

Blockchain complicates how consumer data is managed as the technology's design conflicts with key data protection principles such as data minimisation and the right to withdraw consent. Once a consumer's data is recorded on a blockchain, it becomes difficult to delete or amend, complicating the exercise of data rights such as withdrawing consent or requesting data correction, as provided in the DPA.[319] This immutability raises fundamental questions about the flexibility of such systems. Regulators may need to explore hybrid consent models that allow for the revocability of personal data while maintaining blockchain's security benefits such as through off-chain storage solutions or zero-knowledge proofs, which is particularly evident in the Worldcoin controversy. Worldcoin was poised to be an innovative solution towards the use of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) using unique iris scans and issues a digital identity known as a World ID.

---

317 Addy Wilhelmina *et al., AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analysis*, (n 288), 122.

318 Mousmi Goel, Dr. Amit Verma, Dr. Gurdip Singh, Dr. Nirmesh Sharma, *Blockchain Technology –A Way for Secure Data Storage In Digital Consulting Platforms*, (Vol. 17, No. 1 (I), January – March 2023), 55.

319 Mousmi Goel *et al.*, *Blockchain Technology –A Way for Secure Data Storage In Digital Consulting Platforms*, (n 315) 60.

The World ID was defined not as the user's biometric data, but an identifier created using a cryptography method known as zero-knowledge proofs.[320]

With its decentralised and immutable architecture, blockchain technology has ushered in a new era of transparency, security, and efficiency in data management and transactions.[321] Its potential to revolutionise various sectors - from finance to healthcare - is indisputable. However, the very characteristics that endow blockchain with its power also pose significant challenges, particularly regarding innovation and regulatory compliance. The immutable nature of blockchain data, while enhancing security, can conflict with essential data protection principles, especially those related to informed consent and the right to amend or withdraw personal information.[322] As we delve into the complexities of blockchain's impact, it is essential to recognise how these challenges might impede its wider adoption and integration into existing systems.

The first challenge posed by blockchain it that of decentralisation and authority. In this regard, blockchain technology functions on a decentralised network architecture, which fundamentally distinguishes it from traditional data management systems.[323] In this decentralised model, no single entity possesses complete authoritative control over the data; instead, the oversight and management responsibilities are diffused across a multitude of nodes, contributing to the system's overall integrity and transparency. This contrasts sharply with conventional systems, where roles such as data controllers and processors are explicitly defined, making it easier to assign accountability for data handling and protection.[324] The decentralised nature of blockchain presents significant challenges when it comes to enforcing informed consent from users. In many cases, consumers may find themselves in a position where they are unsure about who is ultimately responsible for processing their personal data. This lack of clarity complicates the process for individuals seeking to voice concerns or grievances regarding their data

---

320 Andrew R. Chow, *What to Know About Worldcoin and the Controversy Around It* (August 2023) https://time.com/6300522/worldcoin-sam-altman/ accessed on 22nd February 2025. See also; Ethreum, *What Are Zero-Knowledge Proofs?*(February 2025) https://ethereum.org/en/zero-knowledge-proofs/ accessed on 22nd February 2025.

321 Mousmi Goel *et al.*, *Blockchain Technology –A Way for Secure Data Storage In Digital Consulting Platforms*, (n 315) 55.

322 Mousmi Goel *et al.*, *Blockchain Technology –A Way for Secure Data Storage In Digital Consulting Platforms*, (n 315) 56.

323 Adil Marouan, Morad Badrani, Nabil Kannouf, and Abdelaziz Chetouanim, 'Blockchain Transformations: Navigating the Decentralized Protocols Era', *Empowering Education: Leveraging Blockchain for Secure Credentials and Lifelong Learning*, (Signals and Communication Technology, Springer, 2024), 1.

324 Adil Marouan *et al.*, , *Empowering Education: Leveraging Blockchain for Secure Credentials and Lifelong Learning*, (n 320) 1.

handling, as they may not know the appropriate party to approach for redress.[325] Moreover, the absence of a central authority or governing body creates additional hurdles in ensuring compliance with established data protection regulations. Without a centralised oversight mechanism, monitoring adherence to legal requirements and consistently safeguarding consumer rights becomes increasingly difficult.[326] This complexity underscores the need for more robust frameworks that can effectively manage accountability and regulatory compliance in decentralised environments.

The second challenge is with respect to smart contracts, which are digital agreements that utilise blockchain technology to automate and optimise various processes, including loan disbursements and penalty enforcement, all without requiring human intervention.[327] This automation enhances efficiency and reduces the potential for errors or fraud that can arise from manual handling. However, a crucial aspect of smart contracts is that once they are deployed onto the blockchain, their operations become immutable, meaning they cannot be altered or revoked. This self-executing nature is a defining feature of smart contracts, allowing them to carry out transactions or enforce agreements automatically based on the predetermined conditions set within the contract code.[328] While this immutability is beneficial in many respects, it can create significant challenges related to the principle of informed consent. Specifically, there are scenarios where consumers may wish to modify the terms of their agreement or withdraw their consent after the contract has been activated.[329] In traditional contract frameworks, parties often have the flexibility to negotiate terms and make amendments as needed. However, in the case of smart contracts, the inability to change the contract after deployment can lead to conflicts and dissatisfaction among users, particularly if their circumstances change or if they feel that the terms are no longer appropriate or fair. This rigidity raises important questions about consumer rights and how to ensure that individuals maintain control over their agreements in an automated environment.

The third challenge pits considerations of transparency against those of privacy. Blockchain technology is often celebrated for its transparency, as it allows transaction records to be

---

325 Carla Reyes, Nizan Geslevich Packin, and Ben Edwards, *Distributed Governance*, (William and Mary Law Review Online: Vol. 59, 2017, Article 1), 7.

326 Abylay Satybaldy, Anushka Subedi, and Sheikh Mohammad Idrees, 'Blockchain Transformations: Navigating the Decentralized Protocols Era', *Empowering Education: Leveraging Blockchain for Secure Credentials and Lifelong Learning*, (Signals and Communication Technology, Springer, 2024), 47.

327 Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, (Ethereum White Paper, 2014), 25

328 ibid (n 326) 25.

329 ibid (n 326) 25.

accessible to anyone on the network. This public visibility can instil trust among users but also raises significant privacy concerns.[330] Even when personally identifiable information (PII) is not explicitly included in blockchain transactions, the metadata associated with those transactions can still disclose sensitive information about individuals.[331] For instance, transaction timestamps, amounts, and patterns can be analysed to infer user habits, financial status, and more details. This kind of analysis can lead to unintended disclosures, potentially putting consumers at risk of identification or exploitation. Moreover, the issue of privacy is exacerbated by the lack of granular consent options in many blockchain implementations.[332] Unlike traditional data systems that often allow users to specify which elements of their data they wish to share or keep private, blockchain systems typically do not provide such flexibility. As a result, consumers frequently find themselves with limited control over how their data is used or who has access to it, leaving them vulnerable in a landscape where their transaction histories could be pieced together to form a comprehensive picture of their activities and preferences.

3.5 Situating the Impact of Speed and Automation in Decision-Making

The integration of automation into credit decisions allows DCPs to process all applications in real-time. While this enhances their efficiency, it may often sideline meaningful consumer engagement in the consent process. Automated systems may present borrowers with pre-determined consent forms, which they are required to accept to access credit, leaving little to no room for negotiation or informed decision-making. This transactional nature further undermines the voluntary nature of consent.[333]

However, the rapidity and autonomation of these processes pose serious challenges to the informed consent model as it exists, as they often prioritise operational efficiencies over consumer understanding and engagement.[334] Regulatory interventions should require that automated systems provide clear, easily accessible explanations of how decisions are made and how data is processed, ensuring that consumers can make informed decisions even in fast-paced lending environments. Speed and automation have been proven to be the core feature of

330 Guy Zyskind, Oz Nathan, and Alex Sandy Pentland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data* (IEEE CS Security and Privacy Workshops, 2015), 181.
331 ibid (n 327) 181.
332 ibid (n 327) 181.
333 Rafe Mazer and Kate McKee, *Focus Note,* (CGAP, Note 108, August 2017), 1.
334 Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent,* (Washington University Law Review, Vol. 96, Issue 6), 1484.

modern digital credit platforms such as M-Shwari. They have enabled the following functionalities to exist as a result.

3.5.1 Instant Credit Approvals

The current automation systems in place enable DCPs to assess a borrower's creditworthiness with remarkable speed, utilising an extensive analysis of pre-collected data sourced from various public domains.[335] This analysis includes information from mobile money transactions, social media interactions, and the borrower's financial activities. This rapid assessment process proves to be especially advantageous for individuals who require urgent financial assistance, including those who are often unbanked and may not have access to traditional banking services.[336] The ability to receive funds quickly can provide critical support to those in immediate need of cash for emergencies, healthcare, or unforeseen expenses.

However, this convenience of instant loan approvals is not without its drawbacks. One significant concern arises from the automated nature of these credit services, which often results in borrowers encountering lengthy and intricate consent agreements during the application process.[337] The fast-paced environment of securing quick funds may leave individuals with little time or motivation to thoroughly read and comprehend the terms and conditions in these agreements. This situation raises important issues regarding the informed consent that is essential under regulatory frameworks, potentially leaving borrowers unaware of the full implications of their financial commitments.

3.5.2 Streamlined Loan Applications

AI-powered chatbots and automated systems play a significant role in guiding borrowers through the intricate credit application process. By streamlining this journey, these technologies greatly minimise the necessity for direct human involvement, which in turn leads to a substantial reduction in both processing costs and the time required to complete applications.[338]

However, implementing such automated systems is not without its drawbacks. One major concern is that they often present borrowers with sets of non-negotiable terms and conditions. This 'take-it-or-leave-it' approach effectively eliminates any opportunity for negotiation or

---

335 ibid (n 333) 1484.

336 Eric Duflos, Juan Carlos Izaguirre, Sai Krishna Kumaraswamy, Laura Brix Newbury, and Myra Valenzuela, *Responsible Digital Financial Ecosystem,* (CGAP, September 2024), 3.

337 Eric Duflos *et al*., *Responsible Digital Financial Ecosystem*, (n 333) 3.

338 Ndung'u Njuguna, *A Digital Financial Services Revolution in Kenya: The M-Pesa Case Study* (African Economic Research Consortium, February 2021), 3.

modification of the terms, which fundamentally undermines the voluntary nature of consent.[339] As a result, consumers may find themselves compelled to accept terms they do not fully understand or agree with to gain access to the credit facility they seek. This dynamic raises serious questions about the ethical implications of the consent process, as individuals are deprived of the ability to opt out of certain data processing activities, further diminishing their agency and control over personal information.[340]

Moreover, the algorithms utilised in AI and ML for automated credit assessment often lack transparency. Borrowers may struggle to comprehend the intricate workings of these technologies, including how their data is analysed and the specific factors that contribute to the approval or rejection of their loan applications.[341] This opacity violates the fundamental principle of informed consent and prevents consumers from making educated decisions regarding their participation in these processes.[342] Additionally, there is a growing concern about algorithmic biases inherent in these systems, which can lead to discriminatory outcomes. Such biases may disproportionately affect certain demographics, exacerbating existing inequalities and further compromising fairness in lending practices.[343] As these issues continue to manifest, it becomes increasingly crucial to address the ethical implications of AI-driven credit systems and to strive for a more transparent and equitable approach to financial services.[344]

3.6 Behavioural Insights and Consent Manipulation

Behavioural insights are increasingly being employed in DCS to influence consumer decision-making. Advanced analytics, for example, derived from frontier technologies allow DCPs to anticipate consumer behaviour, creating opportunities to subtly influence or manipulate consent and subsequently consumer choice and behaviour, creating a vicious cycle.[345] An example is when DCPs frame consent requests in a manner that obscures critical details or

---

339 Neil Richards *et al., The Pathologies of Digital Consent*, (n 331)1479.

340 ibid (n 331)1479.

341 International Telecommunications Union (ITU), *Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective,* (n 26) 19.

342 International Telecommunications Union (ITU), *Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective,* (n 26) 19.

343 Notice Pasipamire and Abton Muroyiwa, *Navigating Algorithm Bias in AI: Ensuring Fairness and Trust in Africa,* (Frontiers in Research Metrics and Analytics, 2024), 2.

344 Nicol Turner Lee, Paul Resnick, and Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms,* (Brookings, Governance Studies Media Office, May 2019).

345 Christina Vasilopoulou, Leonidas Theodorakopoulos, Ioanna Giotopoulos, *Big Data and Consumer Behavior: The Power and Pitfalls of Analytics in the Digital Age*, (Technium Social Sciences Journal, Vol. 45, July 2023), 474.

makes it psychologically difficult for consumers to decline, such as emphasising immediate access to credit at the expense of long-term privacy concerns.[346] This evident exploitation of behavioural tendencies erodes the informed nature of consent and prioritises business interests over consumer protection. Regulators should consider introducing behavioural oversight mechanisms, such as standardising consent formats or requiring consumer testing of consent forms, to ensure clarity and fairness.[347] This may ensure that DCPs are kept accountable for their terms and conditions and any potential changes to these policies. DCPs tend to leverage behavioural insights to influence consumer behaviour during the consent process in two main senses.

The first sense concerns urgency and time pressure. Numerous financial platforms create a misleading perception of urgency by highlighting the rapid approval processes for loan applications.[348] This marketing strategy is particularly detrimental to low-income borrowers, who predominantly use these services. These vulnerable consumers are at heightened risk of behavioural manipulation, as the urgency can cloud their judgment and influence their decision-making.[349] The situation becomes even more complex due to the platforms' design. Many websites feature simplified interfaces that often include pre-selected checkboxes and prominently displayed 'Accept' buttons. While these design choices may be intended to enhance user experience and streamline the application process, they inadvertently contribute to an illusion of efficiency that can reduce the likelihood of borrowers thoroughly reviewing the terms and conditions laid before them.

This practice raises significant concerns about the voluntariness of consumer consent. Many individuals may feel subtly pressured or even coerced into accepting agreements that do not reflect a truly informed or autonomous choice.[350] Moreover, debt collection platforms frequently employ tactics that further amplify this sense of urgency, putting pressure on borrowers to respond immediately. As a result, borrowers may feel they have no alternative but to consent hastily, especially when they are seeking emergency loans to meet pressing financial needs. Such environments create a recipe for exploitation, as the combination of time constraints and a lack of critical engagement with contract details can lead borrowers into

346 Christina Vasilopoulou *et al.*, *Big Data and Consumer Behavior: The Power and Pitfalls of Analytics in the Digital Age*, (n342) 474.
347 ibid (n 333) 3.
348 ibid (n 333) 3.
349 ibid (n 333) 3.
350 ibid (n 333) 3.

unfavourable financial agreements without truly understanding the implications of their commitments.[351]

The second sense involves framing and defaults. In this regard, consent requests are often framed to emphasise the benefits of granting consent while minimising the inherent and potential risks.[352] Furthermore, behavioural insights are employed to structure the consent process so that multiple permissions are combined into a single agreement, making it challenging for consumers to opt out of specific data uses or 'default permissions.'

3.7 Gaps in Regulatory Frameworks

The existing legal framework, including the DPA and the DCP Regulations, lays foundational protections for personal data. However, these laws fall short of addressing the unique challenges posed by emerging frontier technologies, particularly AI. Critical issues such as algorithmic accountability, explainability, and fairness are not sufficiently covered within these existing frameworks, resulting in a regulatory gap. This lag allows Data Service Providers to take advantage of these legislative shortcomings, often leading to negative outcomes for consumers.

Currently, the DPA does not specifically regulate AI-powered credit scoring models, which creates a fertile ground for the proliferation of biases and inaccuracies within these systems. The lack of tailored regulation means that these technologies can operate without rigorous oversight, potentially perpetuating inequality in access to credit and financial services. Addressing this gap is imperative as it will require dynamic regulatory updates to keep pace with technological advancements and an enhancement of the capacities within oversight bodies like the ODPC. Additionally, fostering international collaboration is crucial for tackling the cross-border implications of technological developments.

Moreover, regulatory framework deficiencies are compounded by a significant consumer education and awareness gap. For Kenya to effectively navigate the complexities of a rapidly digitising economy, it must adopt adaptive regulatory practices that respond to the evolving landscape of data use. A critical part of this approach includes prioritising consumer education to ensure that individuals understand their rights and data processing implications.

---

351 ibid (n 333) 3.
352 ibid (n 333) 3.

Implementing policies such as algorithmic audits, which would systematically assess AI models' fairness and accuracy and develop explainable AI frameworks that allow consumers to understand how decisions are made are vital steps in this direction. Additionally, mandating transparency reports from DCPs could bridge the gap between consumer rights and technological practices, fostering greater accountability.

Public awareness campaigns focused on educating consumers about their data rights and privacy issues can empower individuals to make informed choices, creating a more equitable dynamic between DCPs and borrowers. Such initiatives should not be undertaken in isolation; it is essential for regulators, industry stakeholders, and civil society organisations to collaborate in these efforts. This collaborative approach will help ensure that emerging technologies not only enhance consumer protection but also strengthen the informed consent model, allowing consumers to maintain control over their personal information in an increasingly complex digital landscape.

3.8 Conclusion

The regulatory frameworks governing consumer data protection in Kenya's digital credit services (DCSs) underscore the critical importance of safeguarding consumer rights in an increasingly data-driven financial landscape. The Constitution of Kenya, 2010, provides a foundational right to privacy, establishing a robust legal basis for personal data protection. Complementing this, statutes such as the Consumer Protection Act, the Competition Act, and the Data Protection Act (DPA) have introduced specific provisions to ensure transparency, fairness, and accountability in the handling of consumer data by digital credit providers.

Despite these legislative advancements, significant challenges persist. The informed consent model—central to data protection—faces practical limitations due to information asymmetry, opaque algorithmic decision-making processes, and insufficient consumer awareness. Additionally, while regulatory bodies like the Central Bank of Kenya (CBK) play a pivotal role in enforcing compliance, gaps in direct consumer recourse mechanisms and potential systemic inefficiencies hinder effective implementation.

To address these challenges, there is a need for enhanced regulatory oversight, greater transparency in algorithmic processes, and stronger consumer empowerment measures. Reforms such as enabling consumers to directly lodge complaints with oversight bodies like the CBK could improve responsiveness and accountability. Furthermore, fostering public

awareness about data rights and ensuring that service providers adhere to ethical practices will be crucial in building trust and protecting consumers in the dynamic digital credit ecosystem.

In conclusion, while Kenya has made commendable strides in establishing a legal framework for consumer data protection in DCSs, continuous adaptation and enforcement are necessary to keep pace with technological advancements and emerging risks. Strengthening these frameworks will not only safeguard consumer rights but also promote sustainable growth in the digital credit sector.

CHAPTER FOUR
LESSONS FROM SELECTED JURISDICTIONS

4.1 Introduction

That the exponential growth of DCSs has dramatically transformed the landscape of credit access - particularly in markets that have historically been underserved or overlooked by traditional financial institutions - is not in question. These innovative solutions are revolutionising the way individuals and small businesses obtain financing, providing them with opportunities that were previously difficult to realise. Conventional banks often impose rigid eligibility criteria, high fees, and complex processes, creating barriers for many potential borrowers. In contrast, DCSs utilise technology to streamline the loan application process and broaden accessibility, enabling a wider range of consumers to secure credit.

However, alongside this rapid expansion comes a host of challenges, particularly concerning consumer data protection. As DCSs amass and process vast quantities of personal information - from financial histories to biometric data - there is an escalating urgency for strong legal and regulatory frameworks that prioritise the safety and privacy of consumers. The potential for data breaches and misuse of personal information is significant, underscoring the need for robust policies governing how consumer data is collected, stored, and utilised. This chapter offers a comprehensive examination of the regulatory experiences and frameworks established by the EU and South Africa concerning consumer data protection within the digital credit services sector.

By analysing specific laws, guidelines, and enforcement mechanisms developed by these regions, we can gain valuable insights into how they address potential risks and uphold consumer rights in the face of advancing technology. The EU's GDPR serves as a leading example of stringent data protection measures, emphasising principles of transparency, user consent, and the right to data portability. It places significant obligations on organisations to protect personal data and grants individuals' greater control over their information. This framework is designed to protect consumers and foster trust in digital services, which is essential for their sustained usage and growth. Similarly, South Africa has enacted the Protection of Personal Information Act (POPIA), which seeks to balance the privacy rights of individuals with the operational needs of businesses within the digital landscape. POPIA introduces several key provisions aimed at safeguarding personal information while acknowledging the realities of a digital economy. It emphasises accountability and the need for

entities to implement appropriate measures to protect consumer data. By conducting a detailed analysis of the regulatory frameworks in the EU and South Africa, this chapter aims to extract critical lessons and best practices that can be adapted to the Kenyan context. As Kenya experiences a swift increase in the adoption of DCSs - prompted by technological advancements and a growing mobile user base - it is imperative to develop a regulatory approach that not only fosters innovation but also robustly protects consumer data. Ultimately, this chapter aspires to contribute to a deeper understanding of how a well-structured regulatory environment can effectively safeguard consumer interests while facilitating the growth of digital credit services in emerging markets, such as Kenya. Through learning from other jurisdictions.

4.2 Rationale for Selecting the Jurisdictions to Learn From

The decision to examine the EU and South Africa as case studies for comparative analysis in the realm of data protection is rooted in the recognition of their unique yet mutually beneficial approaches. The EU, with its comprehensive GDPR, sets a global benchmark for data privacy and protection, emphasising individual rights and stringent compliance requirements. In contrast, South Africa's POPIA offers a more contextually relevant framework for countries in the Global South, balancing data protection with economic considerations and social dynamics. These regions not only provide valuable insights into the effective governance of personal data but also offer methodologies that can be successfully tailored to fit Kenya's specific socio-economic circumstances. The interplay between regulatory rigour in the EU and the more flexible, adaptive strategies evident in South Africa creates a rich tapestry of practices from which Kenya can draw.

By analysing the legal frameworks, enforcement mechanisms, and cultural attitudes toward data privacy in both jurisdictions, this chapter aims to identify actionable reforms. These reforms will enhance Kenya's legal structure, bringing it in line with recognised international best practices while simultaneously addressing the unique challenges faced within its own domestic landscape. This comprehensive approach ensures that the proposed changes are both feasible and relevant, fostering a robust data protection environment in Kenya.

4.2.1 European Union

The EU has established itself as a preeminent global authority on data protection, largely due to the implementation of its GDPR.[353] This extensive and meticulously crafted legal framework not only sets forth stringent standards for protecting personal data but also embodies a holistic approach that emphasises privacy enhancement and organisational accountability.

At the core of the GDPR are several foundational principles, including lawfulness, transparency, and accountability. These principles serve as a guiding compass, enabling a thoughtful balance between fostering innovation and safeguarding the fundamental rights of individuals. By granting consumers a suite of rights - such as the right to access their data, the right to rectify inaccuracies, and the right to data portability - the GDPR significantly boosts consumer confidence in digital platforms. This, in turn, encourages equitable and meaningful participation in the digital economy, ensuring that individuals can engage in online activities with the assurance that their information is secure and respected.

Moreover, one of the most notable features of the GDPR is its extraterritorial applicability.[354] This provision mandates that organisations located outside of the EU that handle the personal data of EU citizens must comply with the regulation's requirements. This broad reach underscores the GDPR's substantial influence on global data protection practices, shaping how businesses around the world approach data privacy and security.

For countries such as Kenya, examining the EU's framework can provide essential insights into the importance of aligning national legislation with international standards, especially as the digital economy continues to evolve and expand. By investing in a robust legal infrastructure that reflects the principles established by the GDPR, Kenya can better protect its citizens' data and strengthen its position in the global digital landscape.

Kenya's DPA draws heavily on the GDPR, and while it shares many similarities, there are several key differences from which Kenya could learn to further enhance its data protection framework. One major lesson from the GDPR is the importance of robust enforcement mechanisms. The GDPR benefits from a well-established regulatory system, with national data protection authorities working under the guidance of the European Data Protection Board (EDPB) and imposing significant fines for non-compliance. In contrast, Kenya's ODPC is still

[353] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary,* (1st Edition, Oxford University Press, 2020), 2.

[354] General Data Protection Regulations – Regulation (EU) 2016/679, Article 3. See also Christopher Kuner *et al,, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 12 – 13.

developing its capacity and could benefit from additional resources, enhanced independence, and stronger investigative powers. This would not only ensure better compliance but also deter potential violations effectively.

Another important aspect is the harmonization of laws across different sectors. The GDPR applies uniformly across all EU member states, ensuring consistency in data protection practices. Kenya, however, has to navigate overlapping sectoral laws in areas such as banking, health, and telecommunications. A move towards greater legal harmonization could reduce ambiguities and create a more consistent framework for data protection across the board.

The GDPR also stands out in its comprehensive rights granted to data subjects. For example, it explicitly provides for the right to data portability, enabling individuals to easily transfer their personal data between service providers. Although Kenya's DPA also secures rights such as access, correction, and deletion of data, it does not emphasize data portability as strongly. Strengthening this area could be particularly beneficial in sectors like fintech and telecommunications where data fluidity is increasingly important.

International data transfers represent another area where the GDPR sets a high standard. The EU regulation requires that data leaving its jurisdiction is subject to strict safeguards, including mechanisms like standard contractual clauses and binding corporate rules. Kenya's DPA does include provisions for cross-border transfers, but these lack the detailed implementation guidelines found in the GDPR. Learning from the EU's approach could help Kenya refine its rules on international data transfers and ensure a higher level of protection.

Finally, the punitive measures under the GDPR are significantly tougher. With fines reaching up to €20 million or 4% of a company's global turnover, the regulation creates a strong deterrent against non-compliance. In contrast, Kenya's fines—capped at KES 5 million or 1% of annual turnover—may not have the same deterrent effect, especially for larger corporations. Increasing the severity of penalties could be an effective strategy for Kenya to ensure greater adherence to data protection standards.

In summary, while Kenya's DPA provides a strong foundation for protecting personal data, there is ample opportunity to draw lessons from the GDPR. By enhancing enforcement mechanisms, harmonizing legal frameworks, expanding data subject rights such as data portability, refining international data transfer rules, and implementing more robust penalties, Kenya could align its regime more closely with global best practices and better protect its citizens' personal data.

4.2.2 South Africa

South Africa has been chosen as a focal point for comparison due to its relevance as a developing economy that shares both economic structures and cultural traits with Kenya. This comparative analysis is particularly significant given South Africa's advanced and progressive stance on data protection, which stands in contrast to the regulatory frameworks seen in the EU. At the heart of South Africa's efforts is the POPIA, which exemplifies a sophisticated initiative aimed at aligning international best practices in data protection with the specific needs and contexts of local environments. POPIA addresses critical issues such as the digital literacy gap that many consumers face, as well as issues related to financial inclusion, which remain pressing concerns in both nations. Both South Africa and Kenya demonstrate a significant reliance on mobile technologies for conducting financial transactions, culminating in a rapidly evolving digital credit ecosystem. This reliance on mobile platforms underscores the crucial similarities between the two countries, making South Africa an especially relevant case study for Kenya. The primary objective of this thesis is to explore and propose effective strategies for enhancing the legal and regulatory frameworks that govern consumer data protection within DCSs.

Kenya can draw valuable lessons from South Africa's data protection regime, particularly in enforcement, compliance frameworks, and sector-specific regulations. While both countries have data protection laws rooted in similar principles, South Africa has made more progress in implementing and enforcing its regulations.

One of the key differences between the two regimes lies in the strength of their enforcement mechanisms. In South Africa, the Information Regulator (IR) has been actively imposing fines and taking legal action against non-compliant entities. The Protection of Personal Information Act (POPIA) allows for significant penalties, including fines of up to ZAR 10 million (approximately USD 530,000) and potential criminal liability. In contrast, Kenya's Data Protection Act (DPA) imposes a maximum fine of KES 5 million (about USD 38,000), and enforcement by the Office of the Data Protection Commissioner (ODPC) is still in its early stages. Strengthening Kenya's enforcement framework would enhance compliance and deter violations.

Another key area of difference is in cross-border data transfers. While Kenya's DPA requires an adequacy assessment before personal data can be transferred abroad, the implementation of this requirement remains unclear. South Africa, on the other hand, has well-developed

mechanisms for regulating international data transfers, ensuring that personal data is only shared with countries that provide equivalent protection. Kenya could benefit from adopting clearer guidelines and enforcement strategies for cross-border data flows.

South Africa has also made significant progress in developing sector-specific data protection regulations, particularly for industries such as banking, healthcare, and telecommunications. These tailored regulations provide clear compliance guidelines for businesses operating in sensitive sectors. In contrast, Kenya's data protection framework is still evolving, and sector-specific rules are not yet fully developed. Establishing specific regulations for different industries would improve compliance and ensure better protection for sensitive data.

Additionally, South Africa has successfully promoted a culture of public awareness and compliance with data protection laws. The Information Regulator has actively engaged in awareness campaigns and training programs to educate both businesses and individuals about their rights and obligations under POPIA. Kenya's ODPC could adopt a similar approach to enhance public understanding and encourage compliance with data protection laws.

Finally, Kenya could strengthen the investigative powers of the ODPC. In South Africa, the Information Regulator has broad authority to initiate investigations and enforce compliance, even without a formal complaint. In contrast, Kenya's regulator often relies on complaints to take action, which can limit its effectiveness. Expanding the ODPC's authority to proactively investigate potential violations would improve regulatory oversight.

In conclusion, while Kenya's Data Protection Act provides a solid foundation, it can benefit from South Africa's example in key areas such as enforcement, cross-border data transfers, sector-specific regulations, public awareness, and regulatory oversight. By adopting these best practices, Kenya can enhance the effectiveness of its data protection regime and ensure stronger safeguards for personal data.

4.3 Consumer Data Protection in DCSs in the European Union (EU)

The EU exemplifies a global advancement in data protection and privacy regulations., though it is arguable whether it forms the ultimate template from which other jurisdictions should design the data protection frameworks. The GDPR comprehensive and structured regulation addresses a wide spectrum of data protection issues, ranging from collection and processing to storage and erasure of personal data. For nations looking to enhance their data protection frameworks, such as Kenya, the GDPR and decisions arising from its interpretation offer

invaluable insights into developing and implementing effective and forward-thinking legislation. This section delves into the fundamental aspects of the EU's data protection framework, elucidating the core principles and mechanisms that underpin the GDPR, with the ultimate expectation to highlight lessons that Kenya can learn as it ensures data protection in respect of DCSs.

4.3.1 Overview of the EU Framework

The EU's data protection framework is fundamentally anchored in the GDPR, which officially came into effect in May 2018.[355] This regulation serves as a crucial cornerstone of data protection legislation in the EU, establishing a harmonised approach to data privacy across all member states. The GDPR is applicable to a broad range of entities that process the personal data of individuals within the EU, which includes not only traditional organisations but also financial service providers offering DCSs.[356] Its extensive scope covers the entire data lifecycle, encompassing stages from data collection to storage, processing, sharing, and, ultimately, erasure. This comprehensive approach is designed to ensure a high level of consumer protection and to empower individuals with greater control over their personal information. Key principles enshrined in the GDPR comprise several critical elements.[357] Firstly, there is an emphasis on lawfulness, fairness, and transparency, which mandates that data processing be lawful, fair to individuals, and transparent about how and why personal data is used.[358] Secondly, the principle of purpose limitation requires that data be collected for specified, legitimate purposes and not processed in a manner incompatible with those initial purposes.[359] Thirdly, the GDPR advocates for data minimisation, stipulating that only the personal data necessary for processing should be collected.[360] Lastly, the regulation also underscores the importance of accountability, obligating organisations to demonstrate compliance with these principles and take responsibility for their data-handling practices.[361] Overall, the GDPR represents a significant advancement in data protection legislation, aiming to enhance individuals' privacy rights while holding organisations accountable for safeguarding personal data.

---

[355] Christopher Kuner *et al,, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350), 2.
[356] General Data Protection Regulations – Regulation (EU) 2016/679, Article 1.
[357] General Data Protection Regulations – Regulation (EU) 2016/679, Chapter II.
[358] General Data Protection Regulations – Regulation (EU) 2016/679, Article 5 (1) (a).
[359] General Data Protection Regulations – Regulation (EU) 2016/679, Article 5 (1) (b).
[360] General Data Protection Regulations – Regulation (EU) 2016/679, Article 5 (1) (c).
[361] General Data Protection Regulations – Regulation (EU) 2016/679, Article 5 (2).

4.3.1.1 Lawfulness, Fairness, and Transparency

Data must be managed per legal requirements, emphasising transparency regarding both the methods of data collection and the specific purposes for which the data will be used.[362] This transparency is vital for ensuring that all consumers fully comprehend how their personal information is being handled and the rationale behind its utilisation. The transparency principle stipulates that all communications related to the processing of personal data must be easily accessible to the data subjects[363] - essentially, the consumers themselves - and articulated clearly and straightforwardly.[364] Specifically, this principle requires consumers to be informed of the data controller's identity, which is the entity responsible for determining the means and purposes of processing personal data.[365] Additionally, consumers should be aware of the specific objectives the data processing aims to achieve. It is important that these explanations include other pertinent details that support fair and transparent processing practices. Consumers have the right to request confirmation about whether their personal data is being processed, as well as the right to access that data.[366] This aspect of consumer rights aligns closely with Article 6 (1) (a) of the GDPR, which addresses the legitimacy of data processing activities,[367] and Article 12, which emphasises the necessity of providing transparent information about those activities.[368]

> "…The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means…"

---

[362] General Data Protection Regulations – Regulation (EU) 2016/679, Article 5 (1) (a).
[363] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350), 309.
[364] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 309.
[365] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 309.
[366] Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. General Data Protection Regulations – Regulation (EU) 2016/679, Article 6 (1) (a).
[367] Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. General Data Protection Regulations – Regulation (EU) 2016/679, Article 6 (1) (a).
[368] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 314.

However, it is crucial to understand that transparency cannot function independently; it must be reinforced by a commitment to ensuring data processing security, as Article 32 of the GDPR outlines:[369]

> "…Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…"

Moreover, fair data processing implies that information has been collected legitimately, adhering to established legal standards and without any form of deceit or coercion that could leave data subjects unaware of the situation.[370] This concept is intrinsically connected to the principle of transparency, as it emphasises that individuals must be actively informed when their information is being collected.[371] To uphold this, it is essential to provide clear and comprehensible terms and conditions that delineate what types of data are being collected and the purposes for which they are being used. Data subjects must also be informed about the extent of the processing of their data, including how that data may be shared or retained.[372] However, the requirements surrounding these disclosures often do not adequately account for individuals who may possess a limited understanding of complex legal terminologies, underscoring the need for simplification and clarity in communications.

4.3.1.2 Purpose Limitation

Purpose limitation is widely regarded as a cornerstone principle in consumer data protection, particularly under the GDPR framework.[373] This principle mandates that any personal data collected from consumers must be pursued for specific, explicit, and legitimate purposes clearly defined at the outset.[374] As a result, data custodians, along with various financial institutions that offer DCSs, are tasked with the critical responsibility of effectively communicating these purposes to consumers. They must ensure that consumers understand why their data is being collected and grant informed consent.

---

[369] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 314.
[370] Ibid, (n 350) 314.
[371] Ibid (n 350) 314.
[372] Ibid (n 350) 314.
[373] Ibid (n 350) 315.
[374] WP29 2013: Article 29 Working Party, *Opinion 03/2013 on Purpose Limitation* (WP 203, 2 April 2013), 11 – 12.

Processing consumer data for vague, ambiguous, or overly broad purposes can be deemed unlawful if clear definitions regarding the scope of data processing activities are not established.[375] It is imperative that the purposes for which data is being collected are transparent and easily understood by consumers.[376] This clarity ensures that data subjects - individuals whose personal data is collected - are well-informed about the reasons for and methods by which their data will be processed. However, this commitment to clarity poses significant challenges when it comes to the use of black-box algorithms.[377] These complex models often involve intricate data processing methods that even the data handlers may find difficult to interpret. In scenarios such as determining loan classifications or setting interest rates, these algorithms may analyse a multitude of data inputs, but the underlying rationale for the resultant decisions can remain obscured.[378] This lack of transparency raises concerns regarding consumers' ability to fully understand how their data influences critical financial decisions, ultimately complicating the adherence to the principle of purpose limitation in the context of advanced data processing technologies.[379]

4.3.1.3 Data Minimisation

The General Data Protection Regulation (GDPR) employs a rigorous and minimalistic approach to the collection of personal data. One of its core principles is that organisations must limit their data collection solely to what is essential for fulfilling their specified purposes and obligations.[380] This means that businesses are expected to clearly define the reasons for data collection and ensure that any information gathered directly supports those reasons. By enforcing such stringent requirements on data collection, the GDPR significantly reduces the risks associated with data breaches and the potential misuse of personal information - issues that are increasingly prevalent in today's digital landscape. Organisations are compelled to evaluate their data needs critically, which fosters responsible data management practices and enhances accountability.

Moreover, Recital 39 of the GDPR further emphasises the significance of this principle by stating that personal data should only be collected when necessary. This clarification reinforces the regulation's overarching goal of providing stronger protection for individuals' privacy and

[375] Christopher Kuner *et al,, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 315.
[376] General Data Protection Regulations – Regulation (EU) 2016/679, Article 13.
[377] Ibid (n 350) 315.
[378] Ibid (n 350) 315.
[379] Ibid (n 350) 315.
[380] General Data Protection Regulations – Regulation (EU) 2016/679, Article 5 (1) (c).

personal information. By limiting data collection to what is strictly required, the GDPR seeks to create a secure environment where individuals can feel confident that their personal data is safeguarded against unauthorised access and exploitation.

> "…In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review…"[381]

Data minimisation is a critical concept that refers to the quantity of data collected and extends to the duration for which this data is retained. It necessitates the establishment of specific time limits dictating that personal data must be stored only for the minimum period essential for achieving the intended processing purposes. This timeframe should be carefully determined to ensure that it is sufficient to meet legal obligations, fulfil contractual duties, or support legitimate business needs while avoiding the unnecessary and excessive retention of consumer data.[382] By implementing these time constraints, organisations enhance their accountability and transparency, thereby protecting consumer privacy. Such measures serve as a vital safeguard against DCPs that may attempt to exploit consumer data for purposes such as training machine learning models or artificial intelligence algorithms.[383] These safeguards help prevent situations where data is held longer than is ethically or legally warranted, mitigating risks associated with privacy breaches and unauthorised use of sensitive information.[384] It ultimately reinforces the commitment to protecting consumer rights and upholding data protection principles.

Moreover, the GDPR delineates specific rights afforded to individuals, referred to as data subjects. These rights include the ability to access their personal data, ensuring that they can see what information is being held and processed about them. Individuals also have the right to rectify any inaccuracies in their data, which fosters greater trust and ensures that their information remains correct and up to date. Additionally, the GDPR grants individuals the right to request the erasure of their personal data, commonly known as the "right to be forgotten,"

---

[381] Christopher Kuner *et al,, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 310.
[382] General Data Protection Regulations – Regulation (EU) 2016/679, Recital 39.
[383] Lawyers Hub, *Africa Privacy Report 2023/2024*: *A Review of Policy Trends and Digital Frontiers in the Data Protection Landscape,* (January 2023), 21.
[384] Lawyers Hub, *A Review of Policy Trends and Digital Frontiers in the Data Protection Landscape,* (n 380) 21.

which empowers consumers to remove their data from a company's records under certain circumstances.[385] Another significant provision is the right to data portability, which allows individuals to transfer their personal data from one service provider to another seamlessly. This right is particularly important in today's data-centric systems, where users frequently encounter challenges in understanding how their data is collected, processed, and utilised.[386] The complexity of data handling can lead to confusion and privacy concerns among consumers, making these rights essential for enhancing transparency and promoting more informed decision-making regarding personal information.

4.3.1.4 Right to Access

The United Kingdom (UK) Information Commissioner (ICO) reported that 42% of the complaints received in 2017 and 39% of the complaints received in 2018 were about the right of access.[387] This right has two main functions: enhancing transparency and facilitating control.[388] Furthermore, it facilitates effective data control by the subject over the personal data being processed. This allows the data subject to exercise control over their personal data i.e. rectification and erasure pursuant to Article 16 of the GDPR.[389] In 2017, the ICO reported that 42% of the complaints it received were directly related to individuals exercising their right of access to personal data held by organisations.[390] This statistic reflects a growing awareness among individuals about their rights concerning personal data.

The right of access serves several key purposes within data protection legislation. Primarily, it enhances transparency by ensuring that organisations are accountable for how they collect and process personal information.[391] It enables individuals to request information regarding the personal data that organisations hold about them, fostering trust and clarity in the handling of personal data. Moreover, this right equips data subjects with essential tools to assert greater control over their personal information. Individuals can manage their data effectively, which includes not only accessing their data but also exercising their rights to rectification - correcting inaccurate or incomplete information - and erasure, often referred to as the "right to be

---

[385] General Data Protection Regulations – Regulation (EU) 2016/679, Article 17.
[386] Lawyers Hub, *A Review of Policy Trends and Digital Frontiers in the Data Protection Landscape,* (n 380) 21.
[387] ICO 2018B, 30.
[388] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 452.
[389] The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
[390] ICO 2018B, 30.
[391] Christopher Kuner *et al, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 453.

forgotten.[392] These provisions are in accordance with Article 16 of the relevant legislation, which underscores the importance of personal agency in today's data-driven environment. By enabling these rights, the legislation aims to empower individuals to take charge of their personal data, ensuring their privacy and autonomy are upheld in the digital age.

4.3.1.5 Right to Rectification and Erasure

Article 16 of the GDPR epitomises the rights and control that individual, referred to as data subjects, possess over their personal data.[393] This provision is essential to consumer data protection across various legal frameworks, emphasising the importance of individual autonomy concerning personal data management. Specifically, it empowers consumers to correct any false or inaccurate data that may be held about them and enables them to supplement any incomplete information.[394] This provision's rationale stems from the understanding that data completeness may vary depending on the specific context or type of processing involved. For example, while data may fulfil the requirements for one processing purpose, it may be insufficient for another, thereby necessitating the right to obtain more comprehensive data.

Moving to Article 17 of the GDPR, which addresses the right to erasure - often referred to as the "right to be forgotten" - this regulation has generated significant discourse in both academic and legal circles, particularly considering landmark cases such as Google Spain.[395] In this notable case, the court deliberated on whether search engine results should include links to public documents when an individual's name is used as a search term. The ruling concluded that, while the document in question - a publication from a Spanish newspaper - remained publicly accessible, it should not appear in search results associated with the individual's name.[396] This decision critically diminished the publication's 'public impact' on the person involved, raising important questions about privacy and public information accessibility.

However, this case did not comprehensively address all facets of the right to erasure, a gap that was later explored in *Węgrzynowski and Smolczewski v. Poland*.[397] In the aforementioned case, the European Court of Human Rights (ECtHR) ruled that, even if a publication concerning an

[392] Christopher Kuner *et al,, The EU General Data Protection Regulation (GDPR) A Commentary,* (n 350) 452.
[393] Ibid 471.
[394] Ibid (n 350) 473.
[395] Google Spain SL v Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/ 12, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317).
[396] Paragraph 98, Google Spain SL v Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González.
[397] Appeal. No. 33846/ 07, Judgment of 16 July 2013.

individual is found to be erroneous or unlawful, it should remain publicly accessible.[398] This is conditional on the addition of a commentary to the article that informs the audience of the outcomes of any relevant court proceedings. Through this ruling, the ECtHR recognised the inherent risks associated with erasing published materials, likening it to the potential rewriting of historical records.

It is important to note that both aforementioned cases primarily dealt with public records rather than personal data specifically, which is the core focus of this research. Under the parameters of the GDPR, individuals have the unequivocal right to be forgotten concerning their personal data. However, the situation becomes more complex for DCPs, who do not enjoy the same exemptions or protections as traditional publishers like newspapers. Given their handling of personal data, DCPs are required to comply with requests for complete data erasure without exception, maintaining the integrity of consumer privacy rights.

In addition to these rights, the GDPR establishes requirements for Data Protection Impact Assessments (DPIAs) that must be conducted for high-risk processing activities. Examples of such activities include credit scoring or automated decision-making processes utilised by data controllers.[399] DPIAs serve as critical tools for identifying, evaluating, and mitigating potential risks that could adversely affect data subjects, including vulnerabilities related to data breaches or the possibility of arbitrary decisions resulting from opaque algorithms.

Moreover, the GDPR mandates the appointment of Data Protection Officers (DPOs) in organisations involved in extensive data processing activities.[400] This requirement ensures that there is a dedicated resource within the organisation focused on overseeing compliance with the GDPR, fostering a culture of data protection and legal adherence at all organisational levels.

A pivotal aspect of the regulation is its extraterritorial reach, which obligates entities outside the EU that process the personal data of EU citizens to adhere to GDPR standards. This global applicability underscores the regulation's wide-ranging influence on data protection norms and practices in jurisdictions around the world. Such a framework is particularly significant for data controller providers who may be based in one country yet operate across various borders, necessitating compliance with GDPR while navigating differing local regulatory landscapes.[401]

[398] Paragraph 65, Węgrzynowski and Smolczewski v Poland.
[399] General Data Protection Regulations – Regulation (EU) 2016/679, Article 35.
[400] General Data Protection Regulations – Regulation (EU) 2016/679, Guidance Note 97.
[401] General Data Protection Regulations – Regulation (EU) 2016/679, Guidance Note 103 – 104.

4.3.2 Some Salient Lessons from the EU Approach

The EU approach, largely through the GDPR, represents a seminal framework in the data protection domain, safeguarding individuals' rights and freedoms in an increasingly digitised environment. This extensive legislation encompasses numerous aspects. The EU approach empowers individuals and imposes stringent standards on organisations globally. While there are numerous lessons to pick from the EU approach, a few stand out for consideration by countries such as Kenya as it approaches the issue of consumer data protection in the DCSs. Some of these lessons are detailed below.

First, the GDPR significantly enhances consumer trust and engagement by establishing robust rights regarding the handling of personal data. These rights are designed to empower consumers, ensuring they have greater control over their information. For instance, one notable provision is the right to data portability. This right allows consumers to easily transfer their personal data from one service provider to another without the risk of losing access to that information. By enabling such seamless movement, the right to data portability enhances user alternatives and fosters healthy competition within the digital services market. In addition to data portability, another critical aspect of the GDPR is its focus on informed consent. The regulation mandates that organisations obtain explicit consent from consumers before processing their data. This requirement ensures that consumers are fully aware of how their data will be used, who will have access to it, and what implications this may have for their privacy. By promoting transparency and requiring companies to communicate their data practices clearly, the GDPR empowers consumers to make informed decisions regarding their personal information. Kenya could consider adopting similar provisions to enhance consumer rights and protections in the digital ecosystem. By implementing these measures, the country would align itself with international standards and foster a more competitive and trust-based digital services market.

Second, the EU approach strongly emphasises guiding principles rather than strict, inflexible rules. This adaptive approach allows the regulation to remain relevant and effective in the face of rapid technological advancements and innovations. For Kenya, adopting a progressive regulatory framework modelled after the GDPR could yield significant benefits, particularly in the realm of digital credit services. As the digital landscape continues to evolve at a breakneck pace, it is crucial that Kenya establishes a framework that addresses the challenges currently faced and is agile enough to respond to unforeseen developments in data processing methods and technologies. By implementing such a forward-thinking regulatory structure, the country

can ensure that emerging digital credit services are managed in a way that prioritises consumer protection, data privacy, and ethical use of technology. This proactive stance will help safeguard users while fostering an environment conducive to innovation in the financial sector.

Third, the EU approach has set a benchmark for data protection through its robust and comprehensive regulations prioritising the privacy and security of individuals' personal information. Kenya could significantly enhance its data protection landscape by adopting a similar strategy. Implementing a uniform legislative framework would ensure a cohesive approach across various sectors, including DCSs, which are increasingly integral in today's digital economy. This framework could address inconsistencies in existing laws and fill gaps in the application of data protection measures, thereby fostering a more reliable environment for consumers and businesses. A consistent set of regulations would help streamline processes and foster trust among users, while also providing clear guidelines for organisations on handling personal data responsibly. By prioritising these improvements, Kenya could not only safeguard the privacy of its citizens but also enhance its reputation in the global marketplace as a country committed to upholding high standards of data protection.

Fourth, the EU approach acknowledges and embraces the rapid progression of technology by prioritising fundamental principles rather than imposing inflexible regulations. This adaptable approach is particularly vital in the swiftly changing landscape of digital credit services, where innovative data processing techniques and technologies are continually being introduced. The GDPR encourages a proactive framework that anticipates and addresses potential challenges that may arise from these advancements. By focusing on principles such as transparency, accountability, and user consent, the regulation allows for a more versatile application that can respond to unforeseen circumstances effectively. This flexibility is crucial for ensuring consumer protection and fostering an environment that promotes innovation within the digital credit sector, enabling businesses to leverage new technologies while still adhering to essential data privacy and protection standards.

Fifth, the extraterritorial application of data protection regulations within the European Union framework is a significant aspect that ensures foreign entities handling the data of EU citizens are required to adhere to the same stringent standards as local organisations. This means that any company, regardless of its origin, must comply with EU data protection laws when it processes the personal information of EU residents. This regulatory approach reinforces the protection of individuals' privacy rights and fosters a uniform standard for data management

across borders. Kenya has a unique opportunity to follow this model and establish its own international precedent in data protection. By implementing legislation that mandates compliance from global service providers operating within its borders, Kenya can take proactive steps to protect its citizens' personal information. Such measures would not only enhance the safeguarding of data but also create a more secure environment for consumers in an increasingly globalised digital marketplace.

Sixth, the EU approach enforces a distinctly risk-based approach to regulation, emphasising the importance of identifying and addressing potential vulnerabilities in data protection practices. Central to this approach is the GDPR, which mandates that organisations conduct DPIAs. These assessments serve as a vital tool for organisations, compelling them to proactively locate, analyse, and mitigate any potential risks to data protection before they occur. This proactive methodology is especially critical for DCSs, which often leverage complex predictive algorithms and automated decision-making processes. The intensive use of these technologies poses unique challenges, including the potential for bias and the inadvertent exclusion of vulnerable segments of the population. Thus, aligning data protection laws with strong enforcement mechanisms becomes crucial in safeguarding consumer rights and fostering trust in digital systems. Furthermore, the dynamic nature of the digital landscape necessitates that regulatory frameworks are designed with built-in flexibility and adaptability. This enables them to respond effectively to swiftly evolving risks and challenges within the digital financial services sector. A robust regulatory approach must address current threats and anticipate and adapt to future innovations and potential risks, ensuring that consumer rights are upheld and protected in an increasingly complex digital environment.

4.4 Consumer Data Protection in DCSs in South Africa

South Africa's approach highlights the importance of balancing international best practices with domestic needs, a balance Kenya has seemingly failed to uphold. By addressing gaps in digital literacy and financial inclusion, POPIA demonstrates how data protection frameworks – particularly in Africa – can be tailored to foster trust and participation in digital credit ecosystems. The lessons learned from South Africa highlight the necessity of contextual adaptation, robust institutional oversight and proactive consumer education in crafting effective data protection policies for developing economies. South Africa presents a compelling argument for the importance of data protection in developing economies, particularly within the context of DCS. At the forefront of this initiative is the POPIA, which serves as the cornerstone of South Africa's comprehensive data protection framework. The primary

objective of POPIA is to integrate international best practices in data protection while addressing local challenges such as economic disparities, deficiencies in digital literacy, and limited access to essential financial services. This framework's inherent flexibility allows it to evolve and respond to emerging challenges, positioning it as a potential model for other countries in the region, including Kenya.

The implementation of POPIA has been executed in phases, a strategy that has significantly contributed to its acceptance among various stakeholders, including businesses and consumers.[402] This carefully planned rollout has enabled organisations to gradually familiarise themselves with new compliance requirements, significantly minimising potential disruptions to their operations. The phased approach has facilitated a smoother transition into the evolving regulatory landscape by providing businesses with adequate time to realign their processes. Establishing an independent regulatory authority tasked with enforcing POPIA has proven crucial, as it provides oversight for the framework while simultaneously cultivating public and investor confidence in the data protection mechanisms.[403]

In the context of DCS, POPIA addresses several critical issues, including the necessity for obtaining informed consent, ensuring robust data security, and safeguarding the rights of individuals whose personal data is collected and processed. The provisions within POPIA mandate that organisations collect personal information in strict adherence to established data protection principles. Additionally, the Act enforces stringent security protocols designed to protect sensitive consumer information from potential breaches or misuse. These protocols are particularly vital in an expanding digital credit industry, where fostering consumer trust is essential for encouraging broader participation.

Another critical element of South Africa's data protection strategy is its commitment to enhancing public awareness and educating citizens about their rights under the data protection legislation. Recognising that many consumers remain unaware of their rights, the regulatory body has initiated various programs aimed at improving digital literacy across the

[402] Information Regulator (South Africa), *Commencement of Certain Sections of the Act* -< https://www.gov.za/sites/default/files/gcis_document/202104/44383gon297.pdf>- accessed on 22 January 2025.

[403] Grant Williams, Tyron Fourie, Sibulele Siyaya, *The newly enacted Cybercrimes Act and what it means for South Africans,* (GoLegal 26 July 2021) -< https://www.golegal.co.za/newly-enacted-cybercrimes-act/>- accessed on the 22nd January 2025.

population.[404] This strategy bolsters individual rights by empowering consumers with knowledge and encourages businesses to adopt responsible data management practices.

South Africa's approach highlights the essential need to harmonise international best practices with the unique local realities and demands faced by developing economies.[405] This balance appears to be challenging for Kenya and others in the region. By tackling issues related to digital literacy and financial accessibility, POPIA serves as a prime example of how data protection frameworks in Africa can be tailored to reinforce trust and engagement within digital credit systems. Insights drawn from South Africa underscore the significance of contextual adaptability, robust institutional oversight, and proactive consumer education as fundamental components in crafting effective data protection policies for emerging economies. This comprehensive approach safeguards consumer data and enhances the integrity and functionality of digital financial systems.

4.4.1 Overview of South Africa's Legal and Regulatory Framework

South Africa's POPIA, which was enacted in 2013 and became fully operational in 2021, establishes a comprehensive framework for regulating the processing of personal data across various sectors, including in DCSs. POPIA is built upon six fundamental principles of data protection. The first principle is accountability,[406] which establishes that data controllers have a fundamental responsibility to ensure their data handling practices comply with the POPIA. This principle emphasises the necessity for organisations to take proactive steps in demonstrating their adherence to legal standards, thus fostering transparency and trust in their data practices.

The second principle is processing limitation,[407] which mandates that the collection of personal data must be conducted in a lawful manner and solely for specified legitimate purposes. This ensures that individuals' personal information is collected judiciously, preventing any misuse or unauthorised exploitation of their data.

The third principle is purpose specification,[408] which dictates that personal data can only be processed for clear and legitimate objectives that are explicitly defined at the time of data

[404] Grant Williams, *et al.*, *The newly enacted Cybercrimes Act and what it means for South Africans* (n 400).
[405] Ibid (n 400).
[406] Protection of Personal Information Act 2020, s 5.
[407] Protection of Personal Information Act 2020, s 5.
[408] Protection of Personal Information Act 2020, s 5.

collection. This principle helps eliminate vagueness in data usage, ensuring individuals know how their information will be utilised.

The fourth principle is information quality,[409] which requires organisations to actively maintain the accuracy and up-to-date status of their personal data. This obligation ensures that the information remains reliable and relevant, minimising the risk of errors that could negatively impact individuals.

The fifth principle is security safeguards,[410] which calls for the implementation of appropriate technical and organisational measures to protect personal data from loss, damage, or unauthorised access. This principle emphasises the need for robust security frameworks to secure sensitive information against a wide range of potential threats.

The sixth principle is data subject participation,[411] which is a crucial aspect of data protection. It ensures that individuals have the right to access their personal data and request corrections or updates as needed. This principle empowers individuals to control their information, reinforcing their rights and fostering a sense of autonomy over their personal data.

A further notable strength of POPIA lies in its dual approach to fostering a culture of compliance. The Act enforces stringent penalties for organisations that fail to adhere to its stipulations.[412] Yet, it also emphasises the importance of education and awareness by encouraging businesses to adopt best practices in data handling. Organisations are required to obtain explicit consent from individuals and are tasked with meticulously documenting their compliance efforts. This systematic approach not only aligns with international standards but also addresses the unique challenges faced within the South African context, ensuring that the privacy and protection of personal data are taken seriously.[413]

4.4.2 Lessons from the South African Approach

Several lessons abound from the South African approach. The first lesson underscores the significance of contextual adaptation in the realm of data protection laws. In this regard, the

---

409 Protection of Personal Information Act 2020, s 5.

410 Protection of Personal Information Act 2020, s 5.

411 Protection of Personal Information Act 2020, s 5.

412 Information Regulator, *Media Statement: Infringement Notice And R5 Million Administrative Fine Issued To The Department Of Justice And Constitutional Development For Contravention Of POPIA*, (04th July 2023) - < https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf>- accessed on 22nd January 2025.

413 Information Regulator, *Media Statement: Infringement Notice And R5 Million Administrative Fine Issued To The Department Of Justice And Constitutional Development For Contravention Of POPIA*, (n 409).

POPIA exemplifies South Africa's deliberate initiative to align its legal framework with international best practices while concurrently addressing the unique challenges inherent to a developing economy. POPIA reflects a thoughtful consideration of local conditions, such as resource constraints, socio-economic factors, and cultural differences, ensuring that data protection measures are both effective and practicable for South African entities. In comparison, the GDPR is crafted with advanced economies in mind and provides a framework that can be further tailored to meet the specific needs of each European Union member state. This flexibility allows for localised adaptations while maintaining rigorous data protection standards common across the EU. Conversely, Kenya's approach in adopting the GDPR has been notable in that its Data Protection Act closely mirrors the GDPR almost verbatim, without sufficiently addressing the distinct data protection landscape of the country. This near-direct transposition raises concerns about the adequacy of the law in responding to Kenya's specific challenges, such as limited technological infrastructure and varying levels of awareness about data protection among the population. By neglecting to contextualise the GDPR for its own needs, Kenya risks implementing a framework that may not be fully effective in addressing local data protection issues.

The second lesson underscores the critical role of institutional oversight in maintaining data protection and privacy standards. In this framework, the establishment of the Information Regulator serves as a pivotal development, underscoring the need for a robust and independent authority dedicated to ensuring compliance with the POPIA. This regulatory body is essential for addressing grievances related to data protection and privacy violations. The Information Regulator possesses the necessary authority to thoroughly investigate instances of non-compliance, conducting inquiries into potential breaches of the legislation. In addition to investigating, the regulator has the power to levy fines and impose penalties on entities found to be in violation of POPIA, thus reinforcing accountability among organisations that handle personal data. This capacity not only deters future infractions but also reinforces the seriousness with which personal data must be treated. Moreover, the regulator's role extends beyond enforcement; it plays a significant part in offering guidance tailored to specific sectors. This sector-specific guidance helps organisations navigate the complexities of data protection and fosters best practices, ensuring that all stakeholders are aware of their responsibilities under the law. Furthermore, the Information Regulator actively engages in public education and awareness initiatives. By informing the public about their rights regarding data privacy and instilling a deeper understanding of data protection regulations, the regulator fosters an

environment of transparency and trust. This proactive approach cultivates confidence among consumers in the systems that handle their personal information, ultimately enhancing the integrity and efficacy of data-handling practices across all sectors.

The third lesson underscores the critical significance of incremental implementation in the context of legal frameworks such as the POPIA in South Africa. The phased enforcement strategy employed during POPIA's rollout provided various stakeholders, including businesses, government entities, and the public, with sufficient time to comprehend, internalise, and effectively operationalise its requirements. This gradual approach allowed organisations to make necessary adjustments to their data handling practices, develop training programs, and establish compliance mechanisms in a structured manner. In stark contrast, Kenya chose not to implement a phased approach when enacting its data protection law. Instead, upon the law's introduction, all data handlers were mandated to register within an inflexible set timeframe. This immediate and sweeping expectation caught many organisations off guard and did not allow them the luxury of preparation. The lack of a gradual implementation period has had significant repercussions, leading to numerous data breaches as organisations struggled to meet the compliance demands of the new law. Consequently, there was a marked increase in reports filed with the ODPC, highlighting the widespread challenges faced by data handlers. Furthermore, the absence of a structured rollout with gradual benchmarks has contributed to a culture of complacency among data handlers, many of whom continue to rely on outdated algorithms and practices. This stagnation not only poses risks to data security but also adversely affects consumers, who may find themselves at the mercy of ineffective data protection measures. As such, the lesson illustrates that a phased approach in the implementation of data protection laws is essential to ensure that all stakeholders are adequately prepared and that the overall objectives of the legislation are achieved without compromising consumer safety and trust.

The fourth lesson underscores the critical need for sector-specific data protection guidance. Data privacy legislation, such as the POPIA in South Africa, has developed tailored guidelines that cater to the distinct needs of various industries, particularly in the finance sector. This approach highlights the limitations of a "one-size-fits-all" model for data protection, which often falls short in addressing the unique challenges and risks that different sectors face. A similar strategy has been implemented in Kenya, yet it can be described as "a jack of all trades but a master of none." This characterisation suggests that while Kenya's regulatory framework seeks to cover a broad spectrum of data protection issues, it often fails to delve deeply into

specific problems. As a result, this broad approach may address numerous concerns superficially, yet it struggles to provide effective solutions for individual issues, particularly those that require specialised attention. Sector-specific regulations are indispensable in addressing risks associated with different industries. For example, the financial sector is especially susceptible to issues such as predatory lending practices and unauthorised data sharing. These concerns demand targeted and comprehensive regulatory measures to mitigate their effects effectively. Although the DCP Regulations in Kenya acknowledge the problematic nature of predatory lending, they fall short by not addressing the potential role of algorithms and automated decision-making systems that could exacerbate these harmful practices. Conversely, South Africa's guidelines under POPIA stand out for their clarity and specificity. They provide financial institutions with a structured framework that promotes consistent application of data protection principles throughout the sector. By focusing on the particularities of the financial industry, these guidelines enable institutions to implement more robust data protection strategies, ensuring that the unique challenges they face are effectively managed. This targeted approach ultimately helps to foster a more secure and trustworthy environment for consumers, enhancing overall confidence in the financial system.

The fifth lesson highlights the critical need for consumer-centric measures within the digital credit ecosystem, particularly considering the challenges posed by technological advancements. The POPIA places a considerable emphasis on recognising and addressing consumer vulnerability, acknowledging that many individuals may not fully grasp the complexities of data privacy and digital finance. While the legislation prioritises informed consent as a foundational principle, this thesis argues [414]that this approach is inadequate to tackle the multifaceted issues currently facing consumers in the digital credit arena. Informed consent often assumes a level of understanding and capability that many consumers simply do not possess, especially when it comes to the intricate workings of opaque algorithms that dictate lending decisions and data usage. Moreover, the educational initiatives rolled out by the regulatory authorities have indeed made strides in empowering consumers to better understand their data rights. These initiatives equip individuals with the knowledge necessary to identify and contest potential breaches of their rights[415]. However, this strategy mirrors the act of applying a bandage to a broken dam. While it offers some immediate relief, it does not resolve the underlying problems inherent in a system that relies heavily on complex mechanisms that

[414] Protection of Personal Information Act 2020, chapter 3.
[415] Grant Williams, *et al.*, *The newly enacted Cybercrimes Act and what it means for South Africans* (n 400).

lack transparency. Ultimately, it is evident that informed consent, while a valuable component of data protection, does not sufficiently address the challenges posed by the modern digital landscape. The reliance on this principle alone is insufficient, particularly when it comes to safeguarding consumers against the less visible but significant risks associated with algorithm

4.5 Applicability of the Lessons from the EU and South Africa for Kenya

The lessons derived from the EU and South Africa provide significant insights for Kenya as it continues to enhance its consumer data protection framework. These lessons highlight the necessity for a robust, adaptable, and contextually relevant regulatory framework that effectively balances consumer data protection with the evolving nature of DCSs. An integration of well-tailored international best practices would enable Kenya to address existing challenges while simultaneously fostering innovation and instilling trust within its digital economy.

The GDPR underscores the importance of a comprehensive legislative framework that delineates clear principles, establishes a robust enforcement mechanism, and upholds strong consumer rights. The GDPR's focus on data minimisation, purpose limitation, and accountability provides a pragmatic blueprint for ensuring that data protection measures are not only stringent but also enforceable. Furthermore, the GDPR's extraterritorial applicability serves as a potential model for Kenya in navigating the complexities of cross-border data flows, which are increasingly pertinent in the contemporary, digitised economy.

The POPIA emphasises the necessity of contextual adaptation, particularly within developing countries. The phased implementation strategy adopted by South Africa could be a viable approach for Kenya, as it allows for a gradual enforcement process during which businesses and institutions can modify their services and algorithms to align with the new regulatory framework. Additionally, POPIA's commitment to public awareness and digital literacy significantly enhances the roadmap for empowering consumers to understand and effectively exercise their data protection rights.

Kenya must acknowledge its unique challenges, which include gaps in institutional capacity, a limited public awareness concerning data protection issues, and the rapid expansion of DCS without adequate sector-specific guidelines before applying these lessons. By proactively addressing these gaps, Kenya stands to establish a robust legal and regulatory framework that not only meets its local needs but also aligns with international best practices.

Kenya's data protection landscape is primarily governed by the DPA, which draws considerable inspiration from global standards, particularly the GDPR. While the Data Protection Act incorporates numerous principles akin to those of the GDPR and POPIA, significant enforcement gaps and the absence of sector-specific guidelines for DCS remain apparent. The swift growth of Kenya's DCS sector necessitates immediate and effective regulation to safeguard consumers and cultivate trust.

A key lesson that Kenya can extract from the EU is the importance of a comprehensive legislative framework that articulates detailed and enforceable rules. The GDPR's clear emphasis on consumer rights, such as access and data portability, can significantly inform Kenya's approach to consumer empowerment. Additionally, the EU's enforcement mechanisms - such as the imposition of fines and the establishment of independent supervisory authorities - underscore the critical need for strong institutions to ensure compliance. Despite the presence of the ODPC and the imposition of fines on offenders, Kenya's enforcement standards still fall short of global benchmarks.

From South Africa, Kenya can glean the significance of contextual adaptation. The phased implementation of POPIA exemplifies the effectiveness of gradual enforcement, permitting stakeholders to progressively align with the law. This strategy facilitates a comprehensive understanding of the law's implications on daily life rather than imposing abrupt legislative mandates. Furthermore, South Africa's emphasis on consumer education and awareness campaigns highlights the necessity for initiatives designed to enhance public comprehension of data rights, particularly in rural areas where digital literacy may be lacking.

Strengthening Kenya's institutional capacity to enforce the Data Protection Act remains a critical area for development. Enhancing the ODPC with adequate resources, technical expertise, and autonomy is essential. Moreover, fostering clear collaboration and synergy with the CBK and other regional and international data protection and financial institutions could further elevate the ODPC's capacity to address emerging challenges associated with cross-border data flows and DFS.

In summation, therefore, Kenya's adoption of lessons learned from the EU and South Africa must be accompanied by a steadfast commitment to adapt these strategies to its unique context. By addressing gaps in enforcement and public awareness and focusing on specific sectors, Kenya can establish a resilient consumer data protection framework that promotes innovation.

4.6 Conclusion

In conclusion, examining the EU's GDPR alongside South Africa's POPIA reveals critical insights for Kenya as it refines its data protection framework. A key takeaway from the GDPR is the importance of establishing a comprehensive legislative structure supported by robust enforcement mechanisms. In contrast, the contextual adaptation and phased implementation approach exemplified by POPIA offers a pragmatic model for Kenya to consider. By addressing its specific challenges - such as gaps in institutional capacity and low levels of public awareness - Kenya can develop a resilient and adaptable data protection regime. This framework would not only align with international standards but also foster consumer trust and stimulate innovation within its growing digital economy. The lessons drawn from this analysis, in conjunction with discussions from the preceding chapters, ultimately provide an informed backdrop for drawing conclusions and formulating recommendations for this study – a venture undertaken in Chapter Five of this thesis.

CHAPTER FIVE
CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter consolidates the key insights from the previous chapters discussing consumer data protection in DCSs in Kenya and whether the informed consent model is fit for purpose. It offers an in-depth summary of the findings and situates these within the broader challenges identified throughout this thesis as it delineates the critical observations that have been observed during this research. Furthermore, this chapter outlines actionable recommendations tailored to the mitigation of identified gaps whilst evaluating their practicability. Moreover, it identifies avenues for future research to enhance understanding and inform policy and research interventions in this dynamic area.

5.2 Summary of Major Findings

In the pursuit of refining Kenya's data protection framework, it is imperative to consolidate the critical insights derived from comprehensive analyses and lessons drawn in the preceding chapters. This section delves into the findings and observations that have emerged from the exploration of data protection strategies, focusing specifically on the applicability and effectiveness of the informed consent model within Kenya's dynamic digital landscape. The section summarises the findings based on three elements intrinsic to the hypothesis and the research questions. The first element is the existence and context of a legal and regulatory regime governing consumer data protection rights. The second element concerns the reliance on the informed consent model and the inadequacies arising therefrom. The third element involves possibilities surrounding lessons from the law and practice in other jurisdictions.

5.2.1 Findings Based on the First Element of the Hypothesis and Research Question

This study has revealed that the increasing concerns related to privacy violations and the potential misuse of personal data are the primary motivators driving consumer data protection efforts in DCSs in Kenya. The current legal and regulatory framework - which includes key instruments such as the Constitution of Kenya, the DPA, and the DCP Regulations - has made notable advancements in aligning the country's legislation with international standards.

However, despite these positive developments, the framework still lacks the necessary rigor to fully protect consumers particularly with the advent of frontier technologies such as AI, ML, blockchain, big data analytics, credit automation and behavioural interventions. Persistent

challenges obstruct the effectiveness of this legal framework. One significant issue is the weakness of enforcement mechanisms, which hampers the ability of regulatory bodies to adequately address violations and protect consumer rights. Additionally, there is a troubling lack of consumer awareness regarding their rights and the protections afforded to them under the current regulations. Many consumers remain uninformed about the implications of their data being collected and used, which exacerbates their vulnerability in the digital space. Moreover, the inherent limitations of the informed consent model, including weak enforcement mechanisms and low consumer awareness, and the inherent limitation of the informed consent model, have been a focal point throughout this thesis. While the model is theoretically robust and aims to empower consumers by ensuring that they are fully aware of and consent to how their data will be used, it often falls short in practice. This shortcoming is primarily due to the complexity and legal jargon that consumers typically encounter in terms and conditions. The lack of clarity and transparency in these documents can lead to widespread consent fatigue, where consumers, overwhelmed by lengthy terms, either fail to read or disregard them entirely. Consequently, many individuals end up entering into uninformed agreements regarding their personal data, which undermines the intent of the informed consent model and leaves them unprotected in many instances. Although theoretically robust, the informed consent model is undermined by complex terms and lack of clarity, leading to widespread consent fatigue and uninformed consumer agreements, more so with the emergence of frontier technologies in DCSs.

5.2.2 Findings Based on the Second Element of the Hypothesis and Research Question

This thesis provides a comprehensive analysis of the regulatory framework governing consumer data protection in Kenya, highlighting the limitations of the informed consent model in effectively addressing modern challenges. In particular, it argues that this model falls short in dealing with the complexities introduced by advanced technologies, such as AI and machine learning, which rely heavily on intricate algorithms often characterised by their opaque nature. The rapid integration of these technologies into various sectors has exacerbated the challenges faced by consumers in controlling their personal information. As organisations increasingly utilise black-box algorithms to process vast amounts of data, individuals frequently find themselves in a position where they unknowingly consent to terms and conditions that grant companies extensive rights over their personal data. This consent is often granted without a true understanding of how their data will be used, shared, or analysed, which raises significant ethical concerns. Moreover, the current framework lacks robust mechanisms that allow

consumers to revisit or modify their consent agreements once they have been established. This absence of revisability severely undermines the informed consent model's effectiveness, as it does not provide individuals with the necessary tools to regain control over their data in the face of changing circumstances or evolving data practices. As a result, the thesis underscores the urgent need for a more adaptable and transparent regulatory approach that can better protect consumer rights in an increasingly digital and algorithm-driven landscape. It advocates for reforms that prioritise consumer privacy and autonomy, ensuring that individuals are not only informed but also empowered to manage their data in a rapidly changing technological environment.

5.2.3 Findings Based on the Third Element of the Hypothesis and Research Question

A rudimentary comparison with the EU and South Africa has indicated that Kenya may be lagging behind the global standard of data protection, particularly consumer data protection in DCS due to its rigidity in the face of frontier technologies. It has been evidenced that the EU's dynamic consent framework provides an adaptive approach allowing consumers to continuously manage their data preferences. Similarly, South Africa's POPIA demonstrates the importance of integrating robust enforcement mechanisms with data protection legislation. These select jurisdictions have emphasised transparency, accountability and consumer-centric approaches as the key pillars of ensuring a strong data protection regime, which could inform the evolution of Kenya's data protection framework.

5.3 Conclusion

The observations made in this study have indicated that there is an unprecedented growth in DCS in Kenya, which has outpaced the development of regulatory frameworks (which has been termed the pacing problem). This rapid expansion has introduced significant challenges, including the prevalence of predatory lending practices that exploit consumer vulnerabilities, insufficient consumer education, leaving many unaware of their data rights and gaps in enforcement that allow non-compliant entities to operate unchecked.

While the informed consent model forms the cornerstone of consumer data protection, its practical application is hindered by complexities such as the overwhelming amount of data being processed and consumers' inability to understand or effectively manage their consent. The absence of advanced mechanisms, such as real-time data management tools and privacy-by-design principles, exacerbates these issues, leaving consumers exposed to potential data

misuse and exploitation. Addressing these observations requires a holistic approach that combines legislative reforms, technological advancements, and widespread public education.

In conclusion, while Kenya has made commendable progress in the regulation of consumer data protection through legislation such as the DPA, significant gaps remain in addressing the multifaceted challenges posed by frontier technologies. These technologies, including AI and ML, introduce complexities in data processing and privacy management – that existing frameworks struggle to govern effectively.

The reliance on the informed consent model, although foundational, falls short in practice due to issues such as consent fatigue, inadequate consumer education and the opacity of data handling processes. Strengthening enforcement mechanisms is essential in ensuring compliance and deterrence of malpractice by DCPs. Additionally, raising consumer awareness through targeted educational campaigns will empower individuals to make informed decisions about their data. The adoption of dynamic and granular consent models, coupled with the promotion of privacy-by-design principles, can pave the way for a more robust and consumer-centric data protection environment. By addressing these deficiencies, Kenya stands to build a resilient legal framework that not only safeguards consumer data but also enhances trust and confidence in the digital credit ecosystem.

5.4 Recommendations

This analysis further identifies existing gaps and lays the groundwork for practical recommendations aimed at addressing these shortcomings. Some of the salient recommendations arising from the research findings are highlighted below.

5.4.1 Strengthening Enforcement Mechanisms

To bolster consumer data protection in Kenya, it is crucial to establish a dedicated team to deal with consumer-related data within the ODPC. This specialised unit would play a pivotal role in actively monitoring compliance among DCPs, investigating potential violations of data protection laws, and imposing appropriate penalties for any instances of non-compliance. By providing structured guidance, the department can assist DCPs in enhancing their data-handling practices, thus fostering a culture of accountability and transparency within the sector. Furthermore, the task force should have the capacity to collaborate with other governmental bodies and international organisations concerned with data protection. Through these partnerships, knowledge sharing and best practices can be implemented, ensuring that the framework governing data protection is robust and effective.

5.4.2 Enhancement of Consumer Awareness

To effectively monitor the various DCPs utilising AI and ML to provide DCSs in Kenya, it is vital that the relevant government department receives the necessary authority to collaborate closely with both local and international agencies. This partnership will facilitate the establishment of robust oversight mechanisms ensuring adherence to regulatory standards. In tandem with these regulatory frameworks, launching nationwide public education campaigns on data rights in relation to digital credit would be instrumental. These initiatives should be tailored to engage a diverse spectrum of demographics, from students to senior citizens, promoting enhanced digital literacy throughout the population. By doing so, we can significantly elevate the public's awareness regarding consumer data rights and the intricacies involved in reporting any infractions. These educational efforts must extend beyond merely informing the public about data rights. They should also empower participants by providing them with essential skills to identify and resist predatory lending practices, as well as guidance on the appropriate steps to take when they encounter violations. Utilising a multifaceted approach, including community-based workshops, social media outreach, and traditional media channels such as radio and television, will enhance the campaign's outreach and engagement. This comprehensive strategy will not only raise awareness but also foster a culture of informed digital citizenship among Kenyans, ultimately contributing to a more secure and equitable digital landscape.

5.4.3 Adoption of Dynamic Consent Models

Encouraging DCPs to develop robust systems that empower consumers to manage and update their consent preferences on a continuous basis is crucial for advancing data privacy and security. Implementing legislation that supports this model would enhance its effectiveness significantly. Such legislation would establish a framework that requires DCPs to create intuitive and user-friendly interfaces, enabling consumers to easily monitor how their personal data is being used and to adjust their permission settings in real-time. This user-centric approach would not only streamline the process for consumers but also foster a culture of accountability among DCPs. By facilitating regular updates of consent preferences, consumers would have greater control over their data, leading to an improved trust relationship between individuals and organisations that handle their information. Furthermore, if legislated, this model would mandate DCPs to invest in the necessary technology and resources to ensure these systems are accessible and effective. The overarching goal would be to promote transparency in data handling practices, allowing consumers to make informed decisions about their data

privacy and ensuring their rights are respected. By prioritising the establishment of such systems, we can move towards a more responsible and ethical framework for data management.

5.4.4 Promoting Privacy-by-Design

Integrating privacy considerations into the foundational architecture of digital credit platforms such as Tala or Branch during the design phase could significantly enhance the overall effectiveness and trustworthiness of the DCS ecosystem. This proactive approach would require the incorporation of advanced security algorithms that emphasise data minimisation principles, ensuring that only the essential information is collected and processed. Additionally, developers could focus on creating user-friendly features that allow consumers to interact with the platform in a more intuitive and streamlined manner. By facilitating dynamic consent mechanisms, users would have greater control over their personal data, enabling them to easily grant, modify, or revoke permissions as their circumstances change. This user-centric design could also help eliminate the often tedious and confusing legal jargon typically found in lengthy terms and conditions, which can act as barriers to informed consent. Furthermore, integrating these privacy considerations from the outset could not only enhance user trust but also align the platforms with evolving regulations surrounding data protection, ultimately fostering a more transparent and trustworthy financial ecosystem for all stakeholders involved.

5.4.5 Fostering Cross-Border Cooperation

Engaging in collaboration with international regulatory bodies and various stakeholders is essential for addressing the complex challenges associated with cross-border data flows. This collaborative effort, as evidenced by the ongoing strides to harmonise regional data protection laws as well as cross-border data flows, would greatly enhance the capabilities of the ODPC and other governmental entities in Kenya. By working towards harmonising regulations on a global scale, Kenya can create a more cohesive framework for data governance. Such partnerships will enable Kenya to align its consumer data protection standards with internationally recognised best practices, thus fostering greater trust in its data handling processes. Moreover, this alignment can effectively mitigate the risks associated with global data management, such as data breaches and non-compliance with varying international laws. Ultimately, through these strategic alliances and cooperative initiatives, Kenya can enhance its position within the global digital economy, ensuring robust protection of its citizens' data while promoting responsible data practices.

5.5 Opportunities for Future Research

Given the rapid advancements in DCS and data protection technologies, numerous opportunities exist for further research to refine and enhance regulatory frameworks. Future studies could explore the integration of blockchain technology in consumer data protection, particular in enhancing transparency, security and immutability of digital transactions. Additionally, an in-depth examination of the socio-economic impacts of data protection laws on vulnerable groups, such as low-income borrowers and individuals with limited digital integrity, would be valuable.

Further research could also focus on evaluating the effectiveness of emerging data protection models such as granular and dynamic consent frameworks, in improving consumer control over their personal data. Investigating the interplay between AI, ML and data privacy regulations in the digital credit sector could provide insights into mitigating algorithmic bias and ensuring fair lending practices. Moreover, comparative analyses of international best practices in consumer data protection – such as those in the EU and South Africa – could offer lessons for refining Kenya's (and Africa's) regulatory approaches.

Another area worth exploring is the impact of cross-border data flows on digital credit services and the potential for regional regulatory harmonisation within East Africa, and Africa as a whole. Lastly, research on public awareness and consumer education strategies related to data protection would help policymakers design more effective outreach programs to empower consumers in making informed digital financial decisions.

BIBLIOGRAPHY

Addy W, Ajayi-Nifise A, Bello B, Odeyemi O, Falaiye T, *AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analysis*, (Global Journal of Engineering and Technology Advances, February 2024).

Akerlof G, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism,* (The Quarterly Journal of Economics, Vol. 84, No. 3, 1970).

Anant V, Donchak L, Kaplan J, and Soller H, *The Consumer-Data opportunity and the Privacy Imperative,* (McKinsey and Company, April 2020) https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative accessed on 19th February 2025.

Babikian J, *Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era*, (Law Research Journal, Vol 1, No 2, January 2023).

Baldwin R, Cave M, and Lodge M, *Understanding Regulation: Theory, Strategy, and Practice*, (Oxford University Press, Oxford, 2nd Edition, 2012).

Branch Kenya, 'Branch Kenya | FAQs' (March 2021) -<https://branch.co.ke/faq>- accessed 1 March 2024.

Brynjolfsson E, Hitt L and Kim H, *Strength in Numbers: How Does Data-Driven Decision-Making Affect Firm Performance?* (No 5, 2011).

Buterin V, *A Next-Generation Smart Contract and Decentralized Application Platform*, (Ethereum White Paper, 2014).

Cali C, Wollny L, Minsat A and Saint Martin E*, 'Digital Financial Services',* ' (European Investment Bank, 2021).

Calo R*, Digital Market Manipulation*, (George Washington Law Review, Vol 82, No 4, 2014).

Central Bank of Kenya, Press Release, '*Licencing of Digital Credit Providers,'* (March 2024).https://www.centralbank.go.ke/uploads/press_releases/2069457347_Press%20Release%20%20Licensing%20of%207%20Additional%20Digital%20Credit%20Service%20Providers.pdf accessed on 12th October 2024.

Chow A R, *What to Know About Worldcoin and the Controversy Around It* (August 2023) https://time.com/6300522/worldcoin-sam-altman/ accessed on 22nd February 2025.

Central Bank of Kenya, '*Interest Rates Statistics,'* 'Interest Rates | CBK' (March 2024) <https://www.centralbank.go.ke/statistics/interest-rates/> accessed 1 March 2024.

Competition Authority of Kenya*, Report on the Competition Authority of Kenya Digital Credit Market Inquiry*, (2021), https://www.cak.go.ke/sites/default/files/Digital_Credit_Market_Inquiry_Report_2021.pdf

Costa A, Deb A, and Kubzansky M, *Big Data, Small Credit: The Digital Revolution and Its Impact on Emerging Market Consumers* (Innovations, 10, 2015).

Davis F, *Perceived Usefulness, Perceived Ease Of Use, And User Acceptance Of Information Technology,* (MIS Quarterly, 13(3), 1989).

Dal Bo E*, Regulatory Capture: A Review*, (Oxford Review of Economic Policy, 22, 2, 2006).

DellaVigna S and Malmendier U, *Contract Design and Self-Control: Theory and Evidence*, (Quarterly Journal of Economics, Vol. 119, 2004).

Donovan K, *Mobile Money for Financial Inclusion*, (Mobile Money for Financial Inclusion, Information and Communications For Development).

Dr. Goel M, Dr. Verma A, Dr. Singh G, Dr. Sharma N, *Blockchain Technology –A Way for Secure Data Storage In Digital Consulting Platforms*, (Vol. 17, No. 1 (I), January – March 2023).

Duflos E, Izaguirre J C, Kumaraswamy S K, Newbury L B, and Valenzuela M, *Responsible Digital Financial Ecosystem*, (CGAP, September 2024).

Dwer F, Odero J, and Totolo E, *'Digital Credit Audit Report: Evaluating the Conduct and Practice of Digital Lending in Kenya,'* (Financial Sector Deepening Kenya, September 2019).

Dwer F, Odero J, and Totolo E, *Digital Credit Audit Report: Evaluating the Conduct and Practice of Digital Lending in Kenya,* (Financial Sector Deepening Kenya, September 2019).

Eggimann P and Tamo A, *Taming the Beast: Big Data and the Role of Law,* (Big Data and Privacy: Making Ends Meet, 28; Productivity Commission, "Data Availability and Use,").

Eliaz K and Spiegler R, *Contracting with Diversely Naive Agents*, (The Review of Econmic Studies, Vol. 73, Issue 3, July 2006).

Ethreum, *What Are Zero-Knowledge Proofs?* (February 2025) https://ethereum.org/en/zero-knowledge-proofs/ accessed on 22nd February 2025.

European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Version 2.0, October 2020).

European Data Protection Supervisor, *Opinion 11/2021 on the proposal for a Directive on Consumer Credits,* (August 2021).

Ezrachi A and Stucke M E, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge, MA: Harvard University Press, 2016).

Federal Trade Commission, *FTC to Study Data Broker Industry's Collection and Use of Consumer Data* https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data accessed on 20th February 2025.

Felzmann H, Villaronga E F, Lutz C and Tamo-Larrieux A, *Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns,* (Big Data and Society, January – June 2019).

Financial Sector Deepening, *About Us,* https://www.fsdkenya.org/about-us/who-we-are/ accessed on 27th March 2025.

Gabaix X and Laibson D, *Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets*, (Quarterly Journal of Economics, Vol. 121, May 2006).

Gąsiorkiewicz L and Monkiewicz J, *Digital Finance and the Future of the Global Financial System Disruption and Innovation in Financial Services*, (Routledge, 1st Edition, New York).

Gibson E and Buckley R, *Regulating Digital Financial Services Agents in Developing Countries to Promote Financial Inclusion* (SSRN Electronic Journal, 2015).

Goodman B, and Flaxman S, *European Union Regulations on Algorithmic Decision-Making and a Right to Explanation,* (AI Magazine, Association for the Advancement of Artificial Intelligence, 2017).

Gordon F, *Virginia Eubanks – Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, (New York: Picador, St Martin's Press, Law, Technology and Humans, Vol. 1(1), 2018).

Grubb M, *Overconfident Consumers in the Marketplace*, (Journal of Economic Perspectives, Vol. 29, Issue 4, November 2015).

Greenacre J, *What Regulatory Problems Arise When Fintech Lending Expands into Fledgling Credit Markets?* (Washington University Journal of Law and Policy, Vol. 61, 2020).

GSMA, *State of the Industry Report on Mobile Money,* (2021a).

Hildt E and Laas K, *Informed Consent in Digital Data Management,* (Illinois Institute of Technology, January 2022)

Hull G, *Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data* (Ethics and Information Technology Journal, 17, 2015).

Hurlin C, Pérignon C, *Machine Learning Et Nouvelles Sources De Donnes Pour Le Scoring De Crédit*, (Revue d'économie financière, Technologies et Mutations de l'Activité Financière, 2019).

ICO 2018B.

Information Regulator (South Africa), *Commencement of Certain Sections of the Act* -< https://www.gov.za/sites/default/files/gcis_document/202104/44383gon297.pdf>- accessed on 22 January 2025.

Information Regulator, *Media Statement: Infringement Notice And R5 Million Administrative Fine Issued To The Department Of Justice And Constitutional Development For Contravention Of POPIA*, (04th July 2023) -< https://inforegulator.org.za/wp-

content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf>- accessed on 22nd January 2025.

International Financial Consumer Protection Organisation, *Review of Supervisory Tools for Suitable Consumer Lending Practices*, (FinCoNet Report on Responsible Lending 2014) -<http://www.finconet. org/FinCoNetResponsible-Lending-2014.pdf >- accessed on 11th October 2024.

International Telecommunications Union (ITU), '*Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective,'* (ITU Telecommunication Development Bureau (BDT), Bill and Melinda Gates Foundation, 2016).

Intersoft Consulting, *GDPR Consent,* (July 2023) https://gdpr-info.eu/issues/consent/ accessed on 18th February 2025.

Ivanfanta, *Do We Actually Agree to These Terms and Conditions?* (Data Science W231 | Behind the Data: Humans and Values, Ethical Legal Data Science, July 2021) https://blogs.ischool.berkeley.edu/w231/2021/07/09/do-we-actually-agree-to-these-terms-and-conditions/ accessed on 20th February 2025.

Izaguirre J C, and Mazer R, *How Regulators Can Foster More Responsible Digital Credit,* (CGAP, November 2018).

Kaffenberge M, Totolo E, and Soursourian M, *A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania*, (CGAP, October 2018).

Kamau J, *How National Bank Was Brought To Its Deathbed* (September 2019) https://nation.africa/kenya/news/politics/how-national-bank-was-brought-to-its-deathbed-203802 accessed on 21st February 2025.

Kanerika, *AI Agents in Finance: A New Era of Efficiency and Innovation*, (December 29, 2024). AI Agents in Finance: Role, Benefits, and Future Trends accessed on 12th February 2024.

Kemp K and Buckley R, *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model,* (Georgetown Journal of International Affairs, Vol 18, No. 3, International Engagement on Cyber VII, 2017).

King'ori M, *The Data Protection Act, 2019 as a Tool for Permitting Innovation and Consumer Safety in Kenya's Digital Finance Market*, (CIPIT, February 2020) https://cipit.strathmore.edu/the-

data-protection-act-as-a-tool-for-permitting-innovation-and-consumer-safety-in-kenyas-digital-finance-market/ accessed on 21st February 2025.

Kivuva E, *Kenyan Firms on the Spot for Sharing Customer Data,* (Business Daily, July 2021) Kenyan firms on the spot for sharing customer data - Business Daily accessed on 19th February 2025.

Kuner C, Bygrave L A, Docksey C, *The EU General Data Protection Regulation (GDPR) A Commentary,* (1st Edition, Oxford University Press, 2020).

Larsson S, *Algorithmic Governance and the Need for Consumer Empowerment in Data-Driven Markets,* (Internet Policy Review, Vol. 7, Issue 2, May 2018).

Lauer K, Dias D, and Tarazi M, *Bank Agents: Risk Management, Mitigation, and Supervision,* (CGAP Focus Note No 75, Washington, DC: CGAP, December 2011)

Lawi J, '*CBK Blames Legal Void for Inaction on "rogue" Digital Lenders'* (The Star, December 2023) <https://www.the-star.co.ke/business/kenya/2023-12-05-cbk-blames-legal-void-for-inaction-on-rogue-digital-lenders/> accessed 8 July 2024.

Lawyers Hub, *Africa Privacy Report 2023/2024*: *A Review of Policy Trends and Digital Frontiers in the Data Protection Landscape,* (January 2023).

Lee N T, Resnick P, and Barton G*, Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms,* (Brookings, Governance Studies Media Office, May 2019).

Lyman T, Ivatury G, and Staschen S*, Use of Agents in Branchless Banking for the Poor: Rewards, Risks, and Regulation, CGAP Focus Note No 38*, (Washington, DC: CGAP, October 2006).

Malady L and Buckely R, *Building Consumer Demand for Digital Financial Services – The New Regulatory Frontier,* (CIFR Paper No 035/2014 (25 August 2014).

Mandreoli F, Montangero M, *Data Handling in Science and Technology,* (Chapter 9, Data handling in Science and Technology, 2019).

Marouan A, Badrani M, Kannouf N, and Chetouanim A, 'Blockchain Transformations: Navigating the Decentralized Protocols Era', *Empowering Education: Leveraging*

Blockchain for Secure Credentials and Lifelong Learning, (Signals and Communication Technology, Springer, 2024).

Mazer R and McKee K, *Focus Note,* (CGAP, Note 108, August 2017).

Medine D, *Making the Case for Privacy for the Poor,* (CGAP Blog, November 15, 2016).

Moerel L and Prins C, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things,* (Tilburg Law School, May 25, 2016).

Morey T, Forbath T and Schoop A, *Customer Data: Designing for Transparency and Trust* (Harvard Business Review, Analytics and Data Science, May 2015) https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust accessed on 21st February 2025.

Moric Z, Dakic V, Djekic D and Regvart D, Protection *of Personal Data in the Context of E-Commerce*, (Journal of Cybersecurity and Privacy, Vol.4, September 2024).

Mothibi K and Lazaridis D, *Fintech Digital Platforms – An Investigation into Fintech Digital Platform Activity in South Africa and Their Regulatory Implications: Research Document,* (Financial Sector Conduct Authority, 2021).

Muhammad T, Yaseen A, Shah K, *Empowering Financial Services: The Transformative Impact of AI on FinTech Innovation,* (American Journal of Computing and Engineering, Vol. 7, Issue 4).

Mutete C, Indokhomi D, *Kenya: Regulation of Digital Lenders in Kenya | Bowmans* (April 2022) <https://bowmanslaw.com/insights/kenya-regulation-of-digital-lenders-in-kenya/> accessed 8 July 2024.

Mutung'u G, Third Party Data Sharing: Analysis of the Data Protection Bill, 2019, (CIPIT, October 2019) https://cipit.strathmore.edu/third-party-data-sharing-analysis-of-the-data-protection-bill-2019/ accessed on 19th February 2025.

Mwangi I W and Sichei M, *Determinants of Access to Credit by Individuals in Kenya: A Comparative Analysis of the Kenya National FinAccess Surveys of 2006 and 2009* (European Journal of Business and Management, Vol 3, No. 3) 217.

Mzalendo Trust, *Digital Rights in Kenya Report,* (2019).

National Assembly Hansard Report, 17 October 2019.

Nissenbaum H, *A Contextual Approach to Privacy Online*, (Journal of American Academy of Arts and Sciences, Daedalus, 2011) 38.

Njuguna N, *A Digital Financial Services Revolution in Kenya: The M-Pesa Case Study* (African Economic Research Consortium, February 2021).

Noll R, *Economic Perspectives on the Politics of Regulation*, (Handbook of Industrial Organisation, Vol, 2, 1989).

Office of the Data Protection Commissioner, *Guidance Note for the Communication Sector,* (December 2023).

Office of the Data Protection Commissioner, *Registered Data Handlers,* Registered Data Handlers - Office of the Data Protection Commissioner (ODPC)

Outman D, Mazer R, Warren S, and Blackmon W, *Understanding Consumer Protection Risks Faced by Kenyan Digital Finance Users* (Innovations for Poverty Action, July 2020) https://poverty-action.org/study/understanding-consumer-protection-risks-faced-kenyan-digital-finance-users accessed on 20th February 2025.

Pasipamire N and Muroyiwa A, *Navigating Algorithm Bias in AI: Ensuring Fairness and Trust in Africa,* (Frontiers in Research Metrics and Analytics, 2024).

Patel K, *Credit Card Analytics: A review of Fraud Detection and Risk Assessment Techniques*, (International Journal of Computer Trends and Technology, Vol. 71).

Pazarbasioglu C, Mora A G, Uttamchandani M, Natarajan H, Feyen E and Saal M, *Digital Financial Services*, (World Bank Symposium, 2020).

Peltzman S, *Toward a More General Theory of Regulation*, (Conference on the Economics of Politics and Regulation, Vol. 19, No. 2, 1976).

Pigou A C, *The Economics of Welfare*, (London: Macmillan and Co, 4th Edition, 1932).

Posner R, *Theories of Economic Regulation*, (The Bell Journal of Economics and Management Science, RAND Corporation, Vol. 5, No. 2, 1974).

Ratna S, von Allmen U E, Lahrèche-Révil A, Purva K, Sumiko O, Majid B and Kim B, *The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era*, (Departmental Paper No. 20/09, International Monetary Fund 2020).

Reis O, Eneh N E, Ehimuan B, Anyanwu A, Olorunsogo T and Abrahams T O, *Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement*, (International Journal of Applied Research in Social Sciences, Vol 6, Issue 1, 2024).

Reyes C, Packin N G, and Edwards B, *Distributed Governance*, (William &and Mary Law Review Online: Vol. 59, 2017, Article 1).

Richards N and Hartzog W, *The Pathologies of Digital Consent,* (Washington University Law Review, Vol. 96, Issue 6).

Sabrina D and Christoph S, *Digitalisation and Its Impact on SME Finance In Sub-Saharan Africa: Reviewing The Hype and Actual Developments,* (Discussion Paper No. 4/2020, Deutsches Institut für ntwicklungspolitik, Bonn).

Satybaldy A, Subedi A, and Idrees S M, 'Blockchain Transformations: Navigating the Decentralized Protocols Era', *Empowering Education: Leveraging Blockchain for Secure Credentials and Lifelong Learning*, (Signals and Communication Technology, Springer, 2024).

Scheinin M, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, (A/HRC/17/34, 2009).

Securiti, *What are the Different Types of Consent?*(July 2023) https://securiti.ai/blog/types-of-consent/ accessed on 18th February 2025.

Shao Z, *Big Data Revolution in Finance: Opportunities, Challenges, and Future Trends* (Proceedings of the 2nd International Conference on Management Research and Economic Development).

Sherman J, *Data Brokers and Sensitive Data on U.S. Individuals Threats to American Civil Rights, National Security, and Democracy,* (Dule Sanford, Cyber Policy Program).

Solove D, *Introduction: Privacy Self-Management and the Consent Dilemma* (Harvard Law Review 126).

Spence M, *Job Market Signaling,* (The Quarterly Journal of Economics, Vol. 87, No. 3, 1973).

Stigler G, *The Theory of Economic Regulation*, (The Bell Journal of Economics and Management Science, Vol. 2, No. 1, 1971).

Stiglitz J, *The Theory of "Screening," Education, and the Distribution of Income,* (The American Economic Review, Vol. 65, No. 3, 1975).

Suri T and Jack W, *The Long-Run Poverty and Gender Impacts of Mobile Money* (Sciencemag.org, Vol. 354, 6317, 2016).

Tala Kenya, 'Tala Loans Kenya | Download the Tala Loan App (10M+ Installs)' (March 2024) <https://tala.co.ke/tala-app-download-google-play-store-kenya/> accessed 1 March 2024.

Taneja A, *The Transformative Impact of Artificial Intelligence in Financial Services: Enhancing Decision-Making, Efficiency, and Risk Management*, (International Research Journal of Engineering and Technology, Vol. 11, Issue 07, July 2024).

Tarazi M, and Breloff P, *Regulating Bank Agents, CGAP Focus Note 68,* (Washington, DC: CGAP, March 2011).

Tene O and Polonetsky J, *Big Data for All: Privacy and User Control in the Age of Analytics*, (Northwestern Journal of Technology and Intellectual Property, Vol 11, No 5, April 2013).

Thierer A, *The Pacing Problem and the Future of Technology Regulation: Why Policymakers Must Adapt to a World That's Constantly Innovating,* (Mercatus Centre, George Mason University, Technology and Innovation August 8, 2018).

Tullock G, *The Welfare Costs of Tariffs, Monopolies, and Theft*, (Western Economic Journal, Vol. 5, No. 3, 1967).

Vasilopoulou C, Theodorakopoulos L, Giotopoulos I, *Big Data and Consumer Behavior: The Power and Pitfalls of Analytics in the Digital Age*, (Technium Social Sciences Journal, Vol. 45, July 2023).

Venkatesh V and Davis F, *A theoretical extension of the technology acceptance model: Four longitudinal field studies*, (Management Science, Vol. 46, No. 2, 2000).

Wagner G and Eidenmüller H, *Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences,* (The University of Chicago Law Review, 2024).

Wangari J, *OKash, Loan Application Requirements, Interest Rates, Terms and Conditions - Tuko.Co.Ke'* (Tuko.co.ke, March 30, 2021.) <https://www.tuko.co.ke/288602-okash-loan-application-requirements-interest-rates.html> accessed 1 March 2024.

Williams G, Fourie T, Siyaya S, *The newly enacted Cybercrimes Act and what it means for South Africans,* (GoLegal 26 July 2021) -< https://www.golegal.co.za/newly-enacted-cybercrimes-act/>- accessed on the 22nd January 2025.

WP29 2013: Article 29 Working Party, *Opinion 03/2013 on Purpose Limitation* (WP 203, 2 April 2013).

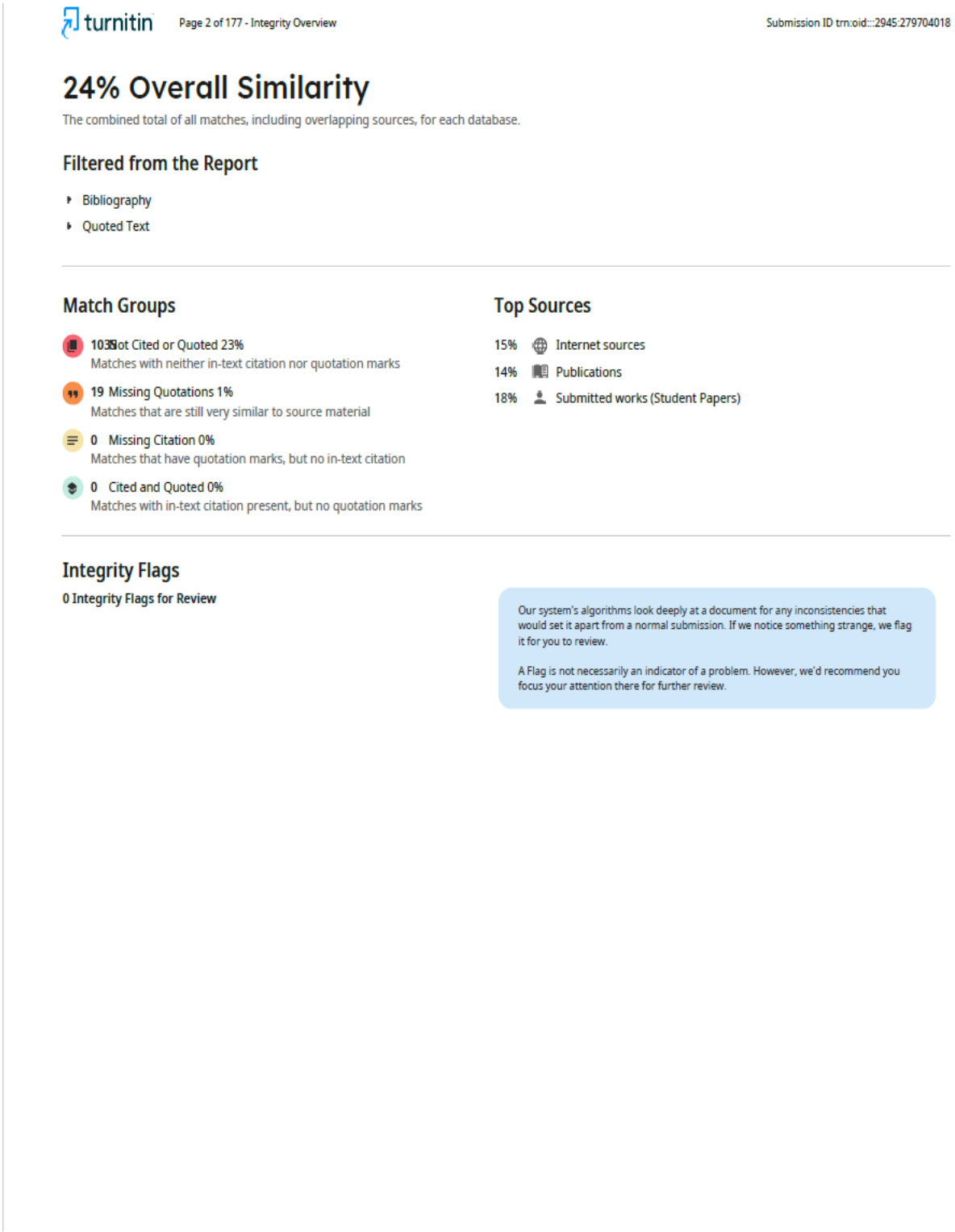
Yaworsky K, Goswami D, and Shrivastava P, *Unlocking the Promise of (Big) Data to Promote Financial Inclusion,* (Accion Global Advisory Solutions, Accion Insights, March 2017).

Zdrok O, *Why "Garbage In, Garbage Out" Should Be the New Mantra for AI Implementation*, (Shelf, May 2024) https://shelf.io/blog/garbage-in-garbage-out-ai-implementation/ accessed on 21st February 2025.

Zyskind G, Nathan O, and Pentland A S, *Decentralizing Privacy: Using Blockchain to Protect Personal Data* (IEEE CS Security and Privacy Workshops, 2015).

APPENDICES

Appendix A: Similarity Report



turnitin Page 2 of 177 - Integrity Overview Submission ID trn:oid:::2945:279704018

24% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

1035 Not Cited or Quoted 23%
Matches with neither in-text citation nor quotation marks

19 Missing Quotations 1%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

15% Internet sources
14% Publications
18% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Appendix B: Ethical Clearance Confirmation

Strathmore UNIVERSITY

26th November 2024

Mr Oundo Jude,
jude.oundo@strathmore.edu

Dear Mr Oundo,

RE: Governing Consumer Data Protection in Digital Credit Services in Kenya: Analysing the Efficacy of Informed Consent in Law

This is to inform you that SU-ISERC has reviewed and **approved** your above **SU-masters** proposal. Your application reference number is **SU-ISERC2462/24.** The approval period is from **26th November 2024 to 25th November 2025.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

Mr Ambrose Rachier,
Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu