2021

Regulation of Fintech: analysis of data protection provisions aimed at protecting consumers in Kenya.

Nyawara, Delbert Ochola
Strathmore Law School
Strathmore University

Regulation of Fintech: Analysis of Data Protection Provisions aimed at Protecting Consumers in Kenya

BY

Delbert Ochola Nyawara

Student Number: 131366

A Thesis Submitted in Partial Fulfillment of the Requirements of the Master of Laws Degree at Strathmore University

Master of Laws

Strathmore University

December, 2021

Declaration

I, Delbert Ochola Nyawara, declare that this thesis which I submit for the degree of Master of Laws at Strathmore University Law School, is my original work and has not previously been submitted for a degree at another university.

Signed…….. Date……

Approval

The thesis of Delbert Ochola Nyawara was reviewed and approved by the following:

Dr. Peter Gitahi Munyi,
Lecturer, Strathmore Law School (Supervisor),
Strathmore University

Dr. Peter Kwenjera,
Dean, Strathmore Law School,
Strathmore University

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

Dedication

This project is dedicated to my parents, Prof. John N. Ochola and Mrs. Grace A. Nyawara, my brother Dr. Anthony N. Ochola and my sister Ms. Brenda A. Nyawara for their positive emotional and financial support while conducting this entire research project and who have always encouraged me to pursue my dreams with passion.

Acknowledgement

First and foremost, I give thanks to the Almighty God for his unending faithfulness.

I acknowledge the support and assistance of Dr. Peter Gitahi Munyi who has guided me throughout this project. He set apart time from his extremely busy schedule, including weekends and public holidays, to peruse my drafts and make invaluable comments and recommendations.

I appreciate the support of my family members who cherish education so much and constantly prayed for me.

I equally acknowledge the support received from G&A Advocates LLP who managed to create a favourable environment for me to conclude this project and I remain indebted to them.

Table of Contents

List of Cases

Olmsted v United States (1938) 277 US Supreme Court

First Bank of Wakeenye v Moden 235 Kan. 260 (1984)

Big Brother Watch and Others v. The United Kingdom [2018] ECHR

Nubian Rights Forum & 2 Others v Attorney General & 6 Others; Child Welfare Society & 9 Others (Interested Parties) [2020] eKLR

Kenya Human Rights Commission v. the Communications Authority of Kenya [2018] eKLR

Vitu Limited vs. The Chief Magistrate Nairobi & Two Others, High Court Misc. Criminal Application No. 475 of 2004

Director of Public Prosecution v Prof. Tom Ojienda & Associates Advocates & 3 Others [2019] eKLR

Abbreviations and Acronyms

FinTech - Financial Technology

RegTech – Regulatory Technology

ECHR – European Convention of Human Rights

UDHR – Universal Declaration of Human Rights

UK – United Kingdom

List of Legislations

Conventions, treaties, protocols and regulations

African Union Convention on Cyber-security and Personal Data Protection, 2014

European General Data Protection Regulation (GDPR) under Directive 2016

International Covenant for Civil and Political Rights, 1966

Universal Declaration of Human Rights, 1948

Kenyan Statutes

Constitution of Kenya, 2010

Competition Act

Central Bank of Kenya Act

Banking Act

National Payment Systems Act

Kenya Information and Communications Act

Capital Markets Act

Consumer Protection Act

Kenya Deposit Insurance Act

The Computer and Cyber Security Act

Data Protection Act (2019)

Abstract

There is no single universal definition of financial technology (Fintech). Fintech can be defined as the delivery of monetary solutions using technology or even the integration and use of technology within finance. The use of Fintech has resulted in a shift in the mode of operation of most financial markets leading to increased opportunities and access to financial services. All the benefits of Fintech aside, Fintech has presented a huge challenge for regulators as there has been lack of clarity in regulation of Fintech leading to various risks being occasioned upon consumers. Additionally, most Fintech solutions do not integrate into the existing regulatory framework leading to more exposure of risk to its consumers, particularly posing risk in the protection of consumer data. In addition, there has been numerous attempts to generate certainty within the existing legal framework for regulation of Fintech. This has been argued to be stifling innovation. To this end, this thesis will assess the regulation of Fintech while protecting the interests of the consumer, particularly on data protection and fostering innovation by analyzing the prevailing regulatory framework in Kenya and across the region while drawing lessons from the United Kingdom on the need for the supervisory authorities to have appropriate mechanisms including investigative and corrective powers.

Chapter One: Introduction

1.1 Background

Financial Technology, or better known as "Fintech" is the delivery of monetary solutions using technology.[1] Fintech can further be defined as a type of combination of technology with a general or specific portion of financial services.[2] Pteja Ivanova in '*Cross-border regulation and fintech: are transnational cooperation agreement the right way to go?*' has also defined Fintech as the utilization information technology in fiscal regimes.[3] In the modern era of digitalization of financial services as compared to prior the development of financial technological infrastructure, Fintech is widely seen as an amalgamation of financial services and information technology.[4] Developments in the financial sector and the technological sector have been deeply intertwined and mutually reinforced.[5] It must be noted that the term Fintech encompasses the entire range of services and activities within the fiscal sector and includes non-bank lenders who more than often, do not fall under the ambits of financial regulation, and therefore moreover do not owe obligations which financial institutions owe such as the fiduciary duty of confidentiality not to disclose customer data.[6]

William Magnuson in '*Regulating FinTech'* argues that Fintech continues to create new challenges to the existing financial regulations.[7] Thus, most regulations in respect to finance and authorities

[1] Douglas W Arner, Janos Barberis and Ross P Buckley, 'The evolution of FinTech: A new post-crisis paradigm,' 47 *Georgetown Journal of International Law*, 2015, 1271.
[2] Anton Didenko, 'Regulating FinTech: Lessons from Africa,' 19 *San Diego International Law Journal,* 2017, 311.
[3] Petja Ivanova, 'Cross-border regulation and fintech: are transnational cooperation agreement the right way to go?' *Uniform Law Review* 24(2), 2019, 367.
[4] Arner *et-al*, 'The evolution of fintech', 1272.
[5] Arner *et-al*, 'the evolution of fintech', 1272
[6] Arner *et-al*, 'the evolution of fintech', 1272
[7] William Magnuson, 'Regulating Fintech' 71 *Vanderbilt Law Review*, 2018, 1167.

are limited in their approach to face the challenges posed by Fintech. It is because of the novelty of Fintech and its mode of operation in business which serious implications on the existing financial regulation. This thesis will therefore seek to set out the unique challenges to financial regulation brought by Fintech in Kenya especially on the protection of consumer data held by Fintech companies and how such challenges can be tackled.

In Kenya, the Capital Markets Authority has published the Regulatory Sandbox Policy Guidance Note which serves the purpose of enabling the entrance of Fintech entities to a Regulatory Sandbox which is basically a unique regulatory environment which permits firms adopting and utilizing innovative products, solutions and services to conduct live tests albeit on a restricted scale.[8] It is expected that the Regulatory Sandbox will assist the CMA to better understand new technology in order to foster an approach to regulation which seeks to promote the objectives of capital markets widening and development thus reinforcing CMA's attempts at increasing its capability to address the impact of novel technology within the capital markets industry.[9]

It is an aim of the Regulatory Sandbox that there will be firm coordination amongst financial industry regulators to guarantee scalable solutions cutting across the board particularly on Fintech. For the Sandbox to work effectively however, there has to be constant communication between the authorities and players within the Fintech Industry.[10] It can therefore be said that the Regulatory Sandbox seeks to foster innovation by giving particular attention on the innovators within the financial sector by allowing them an opportunity within which they can conduct a live testing of

[8] https://kenyanwallstreet.com/cma-publishes-draft-regulatory-sandbox-policy-guidance-notes/ accessed on 17th August 2020

[9] https://kenyanwallstreet.com/cma-publishes-draft-regulatory-sandbox-policy-guidance-notes/ accessed on 17th August 2020

[10] CMA Regulatory Sandbox Policy Guidance Note, March 2019 available on https://www.cma.or.ke/index.php?option=com_content&view=article&id=708:cma-launches-regulatory-sandbox-milestones-report-2&catid=12&Itemid=207 accessed on 14th August 2021.

their products, strengthen the standards of ensuring integrity of information and data while issuing policy options aimed at supporting open networks and updating legal principles that shed more light upon the rights and obligations of parties within the Fintech industry.[11] Whether the sandbox will foster more innovation is simply a test of time.

It has however been argued that the Regulatory Sandbox faces the risk of its participants lacking the requisite knowledge on the operation of new technology and risks that can arise from the new technology even before assessing the new technology in a live environment to safeguard the interests of consumers, thus leading to circumstances where legislation seeking to regulate the new technology is enacted in a limited sector and not across the board thus creating numerous uncertainties for participants within the Fintech industry as well as consumers.[12]

Indeed, the Fintech industry in Kenya led by the mobile banking sector has led to significant legal and regulatory challenges due to its technological character of anonymity, impersonality and being instant.[13] The close relationship in Fintech between telecommunications and mobile banking has further led to risks concerning telecommunications such as technological failure in mobile banking. This is in addition to other risks apart from telecommunications risks such as credit risks, operational risks, systemic risks, fraud and identity risks. These risks are passed on to the consumer as there is no specific mandate under the parent Acts of Parliament for consumer protection beyond

[11] Shulist J, What is the role of regulation in digital finance, 7 August 2018 available on https://www.financedigitalafrica.org/snapshot/what-is-the-role-of-regulation-in-digital-finance/ accessed on 16 August 2020.
[12] Mburu G, 'Case Study Kenya: A regulatory sandbox for the financial sector", published on https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-11/Kenya%20-%20regulatory%20sandbox%20for%20financial%20sector.pdf accessed on 17 August 2020.
[13] Kariuki J, 'Mobile banking Services in the East African Community (EAC):Challenges to the existing legislative and regulatory framework', *4 Journal of Information Policy*, 2014, 272.

the interest of consumers. These parent Acts of Parliament include the Consumer Protection Act[14], the Banking Act[15] and the National Payment Systems Act.[16]

Fintech in Kenya is thus experiencing a rapid growth and thus creates new opportunities through the utilization of data and digital identity.[17] This rapid evolution of Fintech has resulted in new risks due to the sheer amount of data facilities being utilized. Indeed, cyber security risks and tech-based complexity challenge regulatory authorities which are normally trained to deal with traditional financial services.[18] Indeed, the clash of cultures of traditional bankers communicating with Fintech developer may pose risk to the data collected by Fintech firms. Though there are no prohibition on Fintech business in Kenya, the key regulatory authority within the financial sector, being the Central Bank of Kenya, seems to be quite receptive of these innovations.[19]

It must therefore be noted that the relationship between Fintech providers and their customers is created by the general principles of contract which come into being through the creation of a banker-customer relationship.[20] Under a banker-customer relationship, banks are expected to provide secure and reliable banking and payment systems in view of the fiduciary duty of confidentiality bestowed upon them. This duty is however limited to the technical standards within the Bank's immediate control and does not extend to failures in public networks.[21]

[14] Act No. 46 of 2012
[15] Banking Act, Chapter 488 of the Laws of Kenya
[16] Act No. 39 of 2011
[17] Barocas S & Selbst a 'Big data's disparate impact' 104 California Law Review, (2016) 671.
[18] Principles for effective risk data aggregation and risk reporting (2012) available on https://www.bis.org/publ/bcbs239.pdf accessed on 14th August 2021
[19] In 2007, the CBK issued a letter of no objection to Safaricom to operate the MPESA at a time when there was no regulatory framework in place.
[20] Gkoustzinis A, 'Internet banking and the law in Europe: Regulation, Financial integration and Electronic Commerce, *Cambridge University Press*, 2010
[21] Gkoustzinis A, 'Internet banking and the law in Europe: Regulation, Financial integration and Electronic Commerce, *Cambridge University Press*, 2010

Part of this fiduciary duty concerns access control which connotes both a negative and positive obligation which prevents the disclosure of account/consumer information to unauthorized third parties in contravention of the duty of confidentiality and applicable privacy rules.

Additionally, Kenya now has a statute that specifically deals with the handling of personal data being the Data Protection Act.[22] This Act has been framed in such a manner as to give effect to the constitutionally guaranteed right to privacy. The Constitution indeed provides that every person has the right to privacy which also includes the right not to have the information concerning their family and private affairs unnecessarily required or revealed.

The Data Protection Act is applicable to organizations established in foreign jurisdictions but collect data within Kenya as these organizations are expected to give primacy to the right to privacy of the owner when handling this data. Enforcement against these organizations may however be futile especially where these organizations do not have an established legal presence in Kenya and there are no reciprocal enforcement of judgments in Kenya and the host country for those foreign based organizations. Additionally, there are no restrictions on the transfer of data outside Kenya as long as the same is done under the ambit of the right to privacy where the owner of such data grants consent to have the data transferred or stored outside the country.

Despite the above statement of fact, Kenya is in the process of enacting regulations to give effect to the Data Protection Act. These include the Draft Data Protection (Registration of Data Controllers and Processors) Regulations, 2021. Regulation 18 of these Regulations introduce the requirement of registration of data processors which will serve as a means of guaranteeing the safeguards especially for entities which may be located beyond the boundaries of Kenya and which

[22] Act No. 24 of 2019, this Act seeks to regulate the collection and use of personal data.

have access to consumer data in Fintech transactions. It must be noted however that these Regulations are yet to be effected to grant them the full effect of the law.

The use of Fintech has therefore resulted in the spread of data across multiple nodes which may result in the access to private data by third parties and consequently, a violation of data protection laws.[23] The digital transformation of the financial sector therefore requires widespread change in the regulatory approach with a need to update regulations to better facilitate secure access to digitized data, authentication of digital identity and support for core financial service activities such as lending, payments and investment advice.[24]

It must be noted that most Fintech-customer relationships are not necessarily fiduciary relationships.[25] For instance, it is a contractual duty of a banker to a customer which is normally not fiduciary duty except in special circumstances. It therefore follows that as a general principle, and in the usual course of business, the service provider is entitled to prefer its own interests to those of the customer, unlike a trustee or a professional.

Fiduciary duties come into force "*when a person undertakes to perform a service effectively and takes property or accepts power solely for that purpose."*[26] Fintech companies as part of their business engage in the offering of services of making payments on behalf of their consumers. In order to do so, Fintech service providers require consumer financial information which are entrusted upon themselves not to misuse the said transactional data or payment information or abuse the access to that information by misappropriating it and selling it to third-parties. The

[23] Jelena M. 'Fintech Law and Regulation', 16.
[24] Jelena M. 'Fintech Law and Regulation', 16.
[25] Peter Leonard, ' Data Commercialization: contacts, safeguards and no-go zones'
[26] Frankel T. 'Fiduciary duties as default rules', 74 Oregon Law Review, 1209 (1995)

consumers further entrust the Fintech companies to protect their data from loss to other parties. This Fintech-consumer relationship is therefore inherently built on trust. [27]

Fiduciary law as it is, aims at reducing Fintech service providers from misusing their property and further to reduce the costs of monitoring them. Fintech service providers are expected not to betray the trust of their consumers by using their data against them or disclosing their information whether through a data breach or an unauthorized sale to a data vendor.

1.2 Statement of the Problem

Increase in the use of technology in finance has had a great bearing on the Kenyan financial industry. For instance Mobile money, especially M-Pesa by Safaricom, has had the largest impact in the financial industry with an ever-increasing value of mobile transactions with over 96% of households in Kenya using M-Pesa.[28] Online banking together with mobile lending and savings, fundraising platforms, mobile payment systems, peer-to-peer lending and payment platforms, online trading and block chains applications have also gained traction in Kenya resulting in banks changing direction in their mode of operation towards online platforms in banking.

With the more use of technology within financial transactions, and for a really long time, local and international financial institutions which incorporate the use of technology in their financial activities have had a free hand in the collection, collation, analysis and storage of data. These

[27] Sater S, 'Financial Privacy in a Cashles society' April 17, 2019 available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3367610 accessed on 4th May 2021.
[28] Mbiti I, Weil D., 'Mobile Banking: the impact of Mpesa in Kenya, Working Paper No. 2011-13, Brown University, Department of Econommics, Providence, RI (2011). Available on https://www.econstor.eu/bitstream/10419/62662/1/668481188.pdf accessed on 4th May 2021.

institutions now have even higher access to large volumes of private data to which their consumers have no idea is that the entities are trading in their data or using their data for financial gain.

Without adequate enforcement mechanisms there is a great risk that the third party entities that have access to the consumer data will use that consumer data to manipulate the said consumers or discriminate against the said consumers. This would leave the consumers exposed as the third party entities who do not have the consent to access the said data may use the said data to employ underhand tactics against the consumer or even discriminate against the consumer based on certain characteristics obtained from the data.

1.3 Justification of the Study

Fintech is constantly changing the operation of financial markets through the use of technological solutions such as virtual currency, online lending platforms and mobile banking.[29] Indeed, Fintech has led to more unbanked persons to be able to access financial institutions with the increase in online lending platforms within Kenya. With the increasing use of technology in finance, with a legislation in place on data protection being the Data Protection Act and the Consumer Protection Act, which has been termed as being inadequate, there is need to regulate Fintech in a manner that there will be a sufficient data protection framework which will protect the data collected by Fintech firms, given the high likelihood of abuse of data collected by Fintech firms. This also places the consumers of Fintech at a disadvantage as the legal remedies when there are instances of violation of their collected data.

[29] Capgemini, *World FinTech Report* 2017 (2017) 12.

Furthermore, large amounts of personal data collected through various Fintech are stored in servers, networks and mostly electronic filing systems which are found both locally and outside the country.[30] There is therefore a threat that the said data can be accessed by various third parties, both locally and internationally, in a mode which could not be envisaged at the time of collection of data in a Fintech transaction.[31]

The use of technology in traditional systems of finance has undoubtedly resulted in concerns touching on data collection and data privacy. Fintech companies gather a lot of data from their consumers which data is inclusive of sensitive personal data and financial records. Fintech companies also seem to be collecting alternative data which is essentially collection of information touching on a customer's online spending behavior and social media patterns which are required to trace their digital footprint.[32]

Given that the consumer and data protection legal framework in Kenya is underdeveloped, protecting personal data can be attained via the use of well set out data governance methods which focus specifically on the type of financial service being provided. Indeed, digital lenders have been given the leeway to develop, obtain and assess their lending business in comparison to Banks which are highly regulated. There is therefore a need for regulators and Fintech companies to invest in data protection of consumer data with specific focus on regulators drawing the line regarding the protection of consumer data.

[30] Makin P, 'Regulating Issues Around Mobile Banking: New Initiatives to bank the poor are straining the world's financial regulatory systems,' OECD, 2009, 13.
[31] Makin P, 'Regulating Issues Around Mobile Banking: New Initiatives to bank the poor are straining the world's financial regulatory systems,' OECD, 2009, 13.
[32] Claudia NG, Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy, available on https://www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy accessed on 13th December 2020

1.4 Objectives of the Research

The main objective of this thesis will be to find out the most appropriate way to regulate Fintech in Kenya while also protecting the consumer, in particular guaranteeing the protection of consumer data and further fostering innovation within the Fintech industry.

The specific objectives of the thesis will be:

1. To evaluate the current regulatory framework governing Fintech, the banker-customer fiduciary relationship and consumer protection in Kenya;
2. To assess whether there an existing gap on regulation of Fintech and consumer protection in Kenya in relation to the bank-customer relationship which requires the protection of data.
3. To evaluate the regulatory framework in the regulation of Fintech and protection of consumer data in the United Kingdom and draw lessons Kenya can learn from the United Kingdom in order to improve its own regulatory framework.
4. To establish the obstacles to an effective Fintech regulation and protection of consumer data in Kenya.

1.5 Research Questions

The main research question of this thesis will be what is the most appropriate way of regulating Fintech in Kenya while also protecting consumer data within Fintech at the same time fostering innovation.

The specific research questions will be:

1. What is the current regulatory framework regulating Fintech, the banker-customer fiduciary relationship particularly on confidentiality and its effect on protection of consumer data in Kenya?
2. What is the existing gap in the regulation of Fintech and the protection of consumer data in Kenya?
3. What is the regulatory framework in the regulation of Fintech and protection of consumer data in the United Kingdom?
4. What lessons can Kenya draw from the United Kingdom in order to improve its own regulatory framework?
5. What are the obstacles to effective regulation of Fintech and protection of consumer data in Kenya?

1.6 Hypothesis

This thesis will test the following hypotheses:

1. There is an expectation that Fintech service providers are to provide secure and reliable financial systems in view of the fiduciary duty of protection of information and data bestowed upon them.
2. There are increasing incidents phishing of consumer data in Fintech as consumer verification in Fintech has proven difficult to implement due to the fact that Fintech service providers are not regulated in a similar manner as traditional banks.
3. There is little regulation governing the collection, storage and use of personal data which is derived from Fintech transactions.

1.7 Conceptual and Theoretical Framework

Data Protection[33] simply refers to the legal protection of a person (normally referred to as a data subject) with respect to the processing of data concerning that data subject by another person or institution (normally referred to as the data controller).[34] It is widely accepted that the processing of personal information presents a threat to a person's privacy.[35] A person's privacy stands to be violated when another person comes to know of factual private information against that person's will either through an intrusion into the private sphere or through the disclosure of private facts. During data processing, where personal information is gathered thus resulting in knowledge of the same, intrusion naturally occurs.[36] Acts of disclosure, on the other hand, occur when the collected data is thereafter disseminated and consequently disclosed.[37] Another key feature that faces threat through the processing of data is identity.[38] Data processing stands to infringe upon identity when incorrect or misleading data concerning a person is processed.

The theory behind this study can be heavily derived from Samuel Warren and Louis Brandeis' authoritative article "***The Right to Privacy***" in which article it was noted that novel technological advancement served as a threat to privacy and which article further focused on how common law could be used to protect "***privacy***". Warren and Brandeis define privacy as the right to be let alone and in their article attempt to demonstrate that numerous aspects of the right to privacy were in

[33] In certain jurisdictions, the terms 'data privacy' or 'information privacy' are used interchangeably with the term 'data protection' for the reason that the main objective of data protection laws is to protect the interests of the persons involved and not to protect the data itself. Additionally, data protection ought not be confused with data security for the reason that the objects of data protection is to safeguard the interests of individuals particularly where their personal information is processed, while data security principally aims at maintaining confidentiality, integrity and access to information within information systems.

[34] Roos A. Core Principles of data protection law contained in 39 *1The Comparative and International Law Journal of Southern Africa*, 122, (2006).

[35] Bennett Regulating Privacy: data protection and public policy in Europe and the United States (1992) 23

[36] Roos A. Core Principles of data protection law 122 (2006)

[37] Bennett Regulating Privacy: data protection and public policy in Europe and the United States (1992) 23.

[38] Identity can be defined as a person's uniqueness or individuality which identifies or individualizes him as a particular person and thus distinguishes him from others.

existence within the common law. It has however been observed that modern enterprise and invention, which includes the incorporation of technology, have resulted in an invasion of privacy while subjecting individuals to distress which is far greater than could be effected by bodily injury. This sort of harm is not contemplated for under tort law.[39] Later on, Brandeis, as a Supreme Court Justice, rendered a dissenting opinion in the celebrated case of **Olmsted v United States.**[40] In this celebrated case, the Supreme Court found that wiretapping was not a violation of the right to privacy under the Fourth Amendment to the US Constitution as the same did not constitute physical trespass. However, Brandeis, in his dissenting judgment stated that the framers of the United States Constitution "*conferred as against the government the right to be let alone – the most comprehensive of rights and the right most valued by civilized men*." This dissenting opinion demonstrates that the absence of a proper legislative framework on the right to privacy, specifically on data protection in Fintech transactions, might result in harmful violations by the Fintech service providers who act as data controllers.

A second theory that attempts to explain the right to privacy is the Personhood theory. The term "*personhood*" simply refers to those attributes of an individual which are irreducible to his selfhood.[41] This theory seems to suggest that privacy is concerned with the integrity and personality of a person. Prof. Benn has further developed this theory by noting that privacy amounts to "*Respect for someone as a person, as a chooser, implies respect for him as one engaged in a kind of self-creative enterprise which could be disrupted, distorted or frustrated even by so limiting an intrusion as watching*."[42] This points at the importance of consent within privacy, as

[39] Warren S and Brandeis L, "the Right to Privacy" *Harvard Law Review*, 1980, 45.
[40] (1938) 277 US Supreme Court
[41] Freund P, *Privacy: One Concept or Many*, Atherton Press, New York, 1971, 42-43.
[42] Benn S, *Privacy Freedom and Respect for Persons*, Atherton Press, New York, 1971, 26.

individuals should be permitted, under the regulatory framework, to select the type of private information within Fintech transactions, can be shared with third parties and for how long can their person data be held by the Fintech firms and third parties.

This theory attempts to explain the right to privacy. Personhood simply means an individual's attributes which are irreducible to his selfhood.[43] This theory therefore places emphasis on the fact that the protection of consumer data is deeply concerned with the integrity and personality of a person. Indeed, individuals ought to be permitted by law to consent to what type of information can be shared with third parties, at what material time and for what duration of time will such data be vested upon such third parties.

Furthermore, data protection within the Fintech industry ought to be guided by the data protection principles that form the core of protection of the right to privacy.[44] These principles have been enacted as statute within different jurisdictions in respect of data protection within the incorporation of finance in technology in those jurisdictions such as the United Kingdom.

One of the data protection principles is the principle of **accountability**. This principle imposes a duty of care upon data controllers and persons who deal with data within the Fintech sector to take measures to guarantee the processing of such data without infringement of privacy rights of the data subject. This processing is to be carried out in a lawful and reasonable manner.[45] In regard to foreign data subject, given that most Fintech innovations are not bound by geographical boundaries, a data controller or processor is required to ensure that personal data is processed in

[43] Freund P, 'Privacy: One Concept of May,' 42-43
[44] Data Protection Principles available on https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ accessed on 1st March 2021.
[45] Freund P, Privacy: One Concept or Many, 42-43.

compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to this country for processing.

A second principle of data protection is **lawfulness of processing of the captured data**. This principle requires that data ought to only be processed if the purpose, for which it is to be processed, is necessary, relevant and not excessive.[46] This principle goes hand in hand with the concept of consent in that a Fintech provider ought not to process personal data of an individual without the prior consent of the data subject, being the individual whose data is being processed. This however, can be exempted using statute.[47]

One thing that goes hand in hand with this process is the **process of data collection and retention**. It is expected that data collected directly from the data subject should be consented to prior to collection.

In respect of retention, it is expected that data collected should held for periods longer than would be essential for purposes of which data is collected with exceptions being clearly provided for under statute.[48]

Data protection within the Fintech industry further involves the use of data for specific purposes which ought to be properly defined, lawful and related to the activities of the data agent/processor. Additionally, where data is to be harvested by a third party, it is required that such data be used solely for the reason why it had been collected in the first place in order to guarantee that Fintech

[46] The eight data protection principles available on https://vinciworks.com/blog/8-principles-data-protection-act-gdpr-guide/ accessed on 2nd March 2021
[47] See Article 24, Constitution of Kenya, 2010
[48] The Eight Data Protection Principles available on https://www.ed.ac.uk/data-protection/data-protection-policy#:~:text=The%20GDPR%20and%20the%20Act,automated%20decision%2Dmaking%20and%20profiling accessed on 3rd March 2021

entities are open about their reasons for obtaining the personal data, and that what purpose that information serves conforms to the reasonable expectations of the individuals concerned.[49]

Another principle of data protection is the principle of **compatibility of further processing with purpose of collection** which places an obligation among data collectors who hold personal data collected for a specific purpose to guarantee that further processing of the personal data is for that specific purpose.[50] This serves the purpose of guaranteeing that data collectors or data agents/processors cannot use already collected data for another purpose, different from initial purpose, without re-seeking the consent of the data subject.

The data controller has a further obligation to guarantee that the collected data is kept to proper standards in respect of quality through the **principle of quality of information** which principle places an obligation upon data controllers to guarantee that the data in their possession is complete, accurate, up to date and not misleading having regard to the purpose for the collection or processing of the personal data.[51] This is in full conformity with Article 35 of the Constitution which provides that "*every person has the right to the correction or deletion of untrue or misleading information that affects that person*."

A subsequent principle is that of **openness** which requires that data controllers be duly registered by a statutory authority. This principle further places obligations upon data controllers to inform data subjects of the nature of data to be collected, name and address of the person doing the

[49] Processing personal data for specified purposes
[50] The Eight Data Protection Principles available on https://www.ed.ac.uk/data-protection/data-protection-policy#:~:text=The%20GDPR%20and%20the%20Act,automated%20decision%2Dmaking%20and%20profiling accessed on 3rd March 2021
[51] The Eight Data Protection Principles available on https://www.ed.ac.uk/data-protection/data-protection-policy#:~:text=The%20GDPR%20and%20the%20Act,automated%20decision%2Dmaking%20and%20profiling accessed on 3rd March 2021

collection, the purpose of the collection, whether the supply of data is mandatory or voluntary, the consequences of failing to provide data, the provision of law necessitating its collection, the recipients of the data as well as the type of data and who would have the right of access to and the right to request rectification of the data prior to collection.

Therefore, data security safeguards are required to be put I place to require data controllers to take sufficient steps to guarantee the integrity of personal data in the possession or control of a person through the utilization of appropriate, reasonable, technical and effective organizational steps to mitigate against the loss of, damage to, or unauthorized destruction or illicit access to personal data.[52] This places an obligation upon data controllers within the Fintech industry to set up adequate security in respect of their storage system on consumer data which includes firewalls as well as encryption keys and verification models that will militate against exposure of consumer data.

Lastly, the data subject ought to be allowed to **willingly participate** in the processing of collected data that concerns him. This participation includes adequate access to data which is in the possession of the data controller within the Fintech industry or any other third party. It is expected that a data controller will accede to such a request and issue a description of the data it possesses as well as sufficient information concerning the third party who has access to such data. The consumer within the Fintech arena may further require the data controller to provide accurate

[52] The Eight Data Protection Principles available on https://www.ed.ac.uk/data-protection/data-protection-policy#:~:text=The%20GDPR%20and%20the%20Act,automated%20decision%2Dmaking%20and%20profiling accessed on 3rd March 2021

information within its possession and it is expected that the data controller would comply with such a request or at the very least issue credible evidence in support of such data.[53]

It must be noted that **Part IV** of the **Data Protection Act, 2019,** provides for the above principles.[54] The Act, despite outlining the principles, insufficiently delineates on who bears the duty of care in respect of personal data which has already been collected by data collectors but is no longer within their possession, which is what may transpire in various Fintech transactions.

A theory that will be relevant to this study is the Public Interest Theory. This is a philosophical model of regulation with an aim for protecting public interest.[55] Public interest in has further been defined by Johan Den as "*the best possible allocation of scarce resources for individual and collective goods*." This theory of regulation is based on the supposition that unrestrained markets more than often do not succeed due to problems of control and dominations or externalities together with the assumption that governments have the ability to correct market failures through regulation.[56]

It can however be contended that the main perception is that public interest does not have an orderly and accurate formulation and it has been prone to abuse due to its pragmatic and functional definition.[57] Thus, the public interest theory has resulted in a notion that public policy alternative which most warrants implementation, that is, the most attainable standard of administrative action, the baseline of the utmost wisdom or morality in government.[58]

---

[53] The Eight Data Protection Principles available on https://www.ed.ac.uk/data-protection/data-protection-policy#:~:text=The%20GDPR%20and%20the%20Act,automated%20decision%2Dmaking%20and%20profiling accessed on 3rd March 2021

[54] Part IV of the Data Protection Act is concerned with the Principles and Obligations of Personal Data Protection

[55] Johan den Hertog, '*General theories of Regulation, Economic Institute.CLAV*', Utrecht University, 1999.

[56] Shleifer A, 'Understanding Regulation' 11 *European Financial Management*, 2005, 439.

[57] Sorauf F, 'The Public Interest Reconsidered', 19 *The Journal of Politics*, 1957, 616.

[58] Sorauf F, 'The Public Interest Reconsidered' 618.

Centrally in this theory is that the hitches and glitches of a higher and exclusive ethic and wisdom, to which the state is committed to and influences government policy.[59] It is thus the responsibility of the lawmaking and administrative arms of the state to represent the public interest.

A critical evaluation of a public interest is required to commence with a definition and explanation. According to Frank J. Sorauf, there are five central descriptions of the public interest theory which shall form the core of this study. First, Sorauf considers public interest as a shared norm thus, an action could be to mean in the interest of the public as long as it meets the ends of the entire society as opposed to those of a given portion within society.[60] A good number of the proponents of this definition maintain that these shared values and norms must be seriously be held in high regard a majority of the subjects to the authority or at least represent a "consensus" to encompass the desires society.[61] These shared values and norms represent an aspiration of society or the well-being and existence of the state itself.

Secondly, public interest is more than often likened to an interest that controls an exclusive precedence amongst interests due to its superior desirability.[62] The public interest, as a superior desirability arises quite frequently as the consumer interest which ought to be protected.[63]

Thirdly, Sorauf argues that in defence of the citizen who consents to and takes up a complete and unconditional moral standard as a benchmark for person or public action, the recognition of that standard with the public interest follows quite naturally.[64]Sorauf continues to argue that public interest basically embodies the natural law with liberty, fairness, property and unity of mankind

[59] Sorauf F, 'The Public Interest Reconsidered' 619.
[60] Martin Meyerson and Edward C. Banfield, "*Politics, Planning and the Public Interest*" Glencoe, 1955
[61] John Pfiffner and R. Vance Prethus, "Public Administration", 3rd Ed., New York, 1953.
[62] Sorauf F, 'The Public Interest Reconsidered', 619.
[63] Sorauf F, 'The Public Interest Reconsidered', 619.
[64]Sorauf F, 'The Public Interest Reconsidered', 620.

forming public interest. Thus, public interest can be construed to mean "*happiness*" and happiness being given a meaning "*in its strict meaning to moral perfection*."[65]

Fourthly, public interest is also a balance of interests. The public rarely yields entirely to the requirements of a faction of society. Therefore, public interest emerges as the means by which there can be a compromise and accommodation in regulation of various industries.[66]

Finally, it can also be said that public definition is not defined. It can be a yardstick of indefinite length.

Under the Public Interest Theory, efficiency in the distribution of resources is to be attained through government intervention and policy making.[67] Therefore, under this theory, regulation is the means by which shortcomings of flawed competition, unstable market operation, missing markets and detrimental market outcomes can be overcome.[68] It is argued that regulation improves the facilitation and maintenance of market operations.[69]

Therefore, the right to be let alone, as advanced by Warren and Brandeis, alongside the personhood theory, public interest theory and the data protection principles as expounded upon above form the core of the right to information privacy particularly in Fintech transactions. This right places a negative obligation upon the government and other persons or entities to restrain themselves from interfering/intervening in the personal affairs of an individual without that individual's prior consent. Thus, with the rising huge amount of information that is held by telecommunication companies[70], traditional financial institutions such as banks and other data controllers and/or data

[65] Sorauf F, 'The Public Interest Reconsidered', 620.
[66] Sorauf F, 'The Public Interest Reconsidered', 621.
[67] Shleifer A, 'Understanding Regulation', *11 European Financial Management*, 2005, 439.
[68] Shleifer A, 'Understanding Regulation', 439.
[69] Shleifer A, 'Understanding Regulation', 439..
[70] Such as Safaricom through M-Pesa and related platforms

agents' as a direct consequence of the use of more technological platforms in finance in Kenya, there is a huge need to supplement the provisions of the Data Protection Act to provide a sufficient framework that will guide on the protection of consumer data within the Fintech arena.

1.8 Research Methodology

Research methodology is the overall approach to research, including the philosophical and theoretical ideas, and procedures which will be used in the research as well as the methods of analysis of the data collected. The methodology to be used in this research will be mainly be doctrinal in nature and hence with will use desk research methodology to gather data. Doctrinal research methods include the complete interpretation and scrutiny of legal material for instance statute, subsidiary regulations, case law, regulatory guidance, soft law and authoritative legal texts. This methodology is important as it will entail the identification of specific legal rules which will be discussed alongside their underlying principles in order to identify any ambiguities within the law.

The methodology will therefore entail a review of the literature on use of technology in finance, consumer protection and the fiduciary duty owed by banks to protect the data of their customers. This will involve an analysis of court judgments, where the central issue is protection of consumer data in Fintech. A critical review will be done using various books, journal articles, projects, academic papers, academic reports and legislation to examine the historical and current societal and judicial views around the world on the protection of consumer data in Fintech.

The methods of protection of consumer data in Fintech in various countries will also be examined. The best practices will be picked and recommendations on how these practices can be implemented in Kenya will be made. Although this thesis will pick the best practice from various countries,

emphasis will be paid to the United Kingdom. The developments of the issue of protection of consumer data in these two countries will be analyzed.

It is important to explain why the United Kingdom has been selected. The choice of the UK is largely due to historical consideration. Kenya derived the common law system from the UK and precedent from the UK, though not binding, is highly persuasive within the Kenyan legal system.

1.9 Literature Review

Petja Ivanova in '*Cross-Border regulation and Fintech: are transnational cooperation agreements the right way to go?*' Begins by defining what regulation is by stating that it is the governmental standards or directives supported by tough penalties compelling private persons to embark on performing or refrain from specific conduct and within the financial industry, regulation is done at the national, regional and international levels in order to maintain confidence within the fiscal system by giving assurance in legal certainty, precision and predictability and above all preventing systemic failure within the financial industry.[71] Ivanova notes that regulation has four primary methodologies: rule-making, supervision, certification and enforcement through which regulators can opt to directly utilize these approaches or can assign the burden of regulation onto private actors.[72]

In respect to the regulation of Fintech, Ivanova calls for cross-border regulation in order to minimize the disruptive climax under the prevailing financial industry and further to guarantee that the right performance, integrity and productivity of the general financial system.[73] This is because Fintech corporations utilize internet platforms which are not limited to a country's

[71] Petja Ivanova, 'Cross-border regulation and fintech: are transnational cooperation agreement the right way to go?' *Uniform Law Review 24(2)*, 2019, 367.
[72] Ivanova P, 'Cross-border regulation and fintech,' 367.
[73] Ivanova P, 'Cross-border regulation and fintech,' 369.

territorial boundaries to distribute a wider range of financial products and services to the general public while also using a diverse range of features such as automated processes and programming which are fundamental to their trade industry and are likely to propagate shock in case of stress scenarios within the financial industry while circumventing existing intermediaries.[74]

Gordana Golubic acknowledges that technology is deeply embedded in the modern financial sector bringing with it challenges to the established regulatory framework as the influence and the transformative power of digital technology in finance cannot be fully foreseen.[75] Golubic further notes, that the services offered by Fintech firms are not bound by territorial limits and can therefore reach a global market where no regulatory barriers exist.[76] Golubic finally makes the observation that while the main objective of financial regulation is to create a stable market and to safeguard the consumers against losses through the elimination of systemic risk, a technology-driven sector favours self-regulation which affects the timing of imposing regulation on Fintech as the same may affect both inclusion of technology within the financial sector and its further development.[77] Golubic concludes by noting that the existing regulatory framework is neither sufficient nor ready for enforcing rules as rapidly as novel products and services emerge thereby leaving room for manipulation and consumer threats.[78] Golubic therefore sees the need for protection of consumers while drafting regulation covering the Fintech sector.

Douglas W. Arner, Dirk A. Zetsche, Ross P. Buckley and Janos N. Barberis in '*FinTech and RegTech: Enabling Innovation While Preserving Financial Stability'* rightfully assert that Fintech

[74] Ivanova P, 'Cross-border regulation and fintech,' 369,
[75] Golubic G, 'Do Digital Technologies Have the Power to Disrupt Commercial Banking' 6 *InterEULawEast: Journal for International and European Law, Economics and Market Integrations*, 2019, 83.
[76] Golubic G, 'Do Digital Technologies Have the Power to Disrupt Commercial Banking', 84.
[77] Golubic G, 'Do Digital Technologies Have the Power to Disrupt Commercial Banking', 84.
[78] Golubic G, 'Do Digital Technologies Have the Power to Disrupt Commercial Banking', 85.

has in the recent times gained significance forcing various financial regulators to reconsider their approach towards balancing the conventional regulatory objectives of financial stability and consumer protection while still upholding and preserving the intended purposes of growth and innovation.[79] They correctly indicate that the act of balancing conventional regulatory objectives with those of growth and innovation has proved to be a challenge as the regulatory environment is largely focused on preventing disruption rather than encouraging it as is the aim of many Fintech.[80] Arner, Zetsche, Buckley and Barberis further note that technology is increasingly participating in a major way in regulation itself, particularly financial regulation in what has been coined as "RegTech" as regulators have moved from regulations which are calculated to control human conduct to supervision of automated processes. Technology is therefore used under the background of regulation, monitoring, reporting and compliance.[81] Regtech has therefore presented an opportunity to consider regulation more broadly.

Vicki Waye in 'Regtech: *A new Frontier in Legal Scholarship'* equally notes that there is a digital disruption being experienced across a succession of industries while transforming the social, economic and legal landscapes. This has in turn resulted in disruption of specific legal doctrines and practices whole at the same time impacting the means of and the method of engagement between the governor and the governed.[82] The motivating factor for the changes is the intense and complex growth of Fintech which has escalated the costs of regulatory compliance.[83] Thus, to handle and endure the compliance challenge, a considerable amount of automated solutions have

[79] Arner D, Zetzsche D, Buckley R and Barberis J, 'FinTech and RegTech: Enabling Innovation While Preserving Financial Stability', 18 *Georgetown Journal of International Affairs, 2017,* 47.
[80] Arner D *et-al*, 'FinTech and RegTech: Enabling Innovation While Preserving Financial Stability', 49.
[81] Arner D *et-al*, 'FinTech and RegTech: Enabling Innovation While Preserving Financial Stability', 49.
[82] Anagnostopoulos J, 'Fintech and Regtech: Impact on Regulators and Banks" (2018) 100 *November Journal of Economics and Business,* 2018.
[83] Waye v, 'Regtech: A New Frontier in Legal Scholarship', 40 *Adelaide Law Review,* 2019, [ix].

been devised to assist in regulatory compliance under the moniker of "RegTech". Regtech has arising within the financial industry alongside Fintech[84] which has continued to harness digitization to generate novel financial products and services and result in much better efficiencies in current services. [85]

Waye argues that Regtech has been evolving with an increase in the number of sectors it serves as it utilizes mechanisms which comprise of the collation and analysis of big data, natural language processing, relating the analytics with machine learning, the application of distributed ledger technology, and the automation of algorithmic process to speed up and improve compliance and regulation.[86]

William Magnuson opines that the rise of Fintech has occasioned challenges for current financial regulations.[87] This is because recent financial reforms are inadequate in addressing the challenges posed by the Fintech and also suppress helpful and valuable innovation within the financial sector.[88] Magnuson also argues that because of the novelty of Fintech, regulators are only beginning to become accustomed to its effects on financial regulation. He thereafter goes ahead to further an argument that the evolution of fintech has resulted in unique challenges to financial regulation.

Anton Didenko in '*Regulating FinTech: Lessons from Africa'*, in justifying the reason for constant regulation of Fintech notes that FinTech does not enjoy the support of existing regulatory regimes

[84] Puschmann T, "Fintech" (2017) 59(1) Business & Information Systems Engineering 69.
[85] Zetzsche D, et al, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation" *23(1) Fordham Journal of Corporate and Financial Law,* 2017, 31.
[86] Waye V, 'Regtech: A New Frontier in Legal Scholarship' 57.
[87] Magnuson W, 'Regulating Fintech' 71 *Vanderbilt Law Review*, 2018, 1167.
[88] Magnuson W, 'Regulating Fintech', 1172.

even though Fintech gives easy access of financial services to nearly all persons.[89] Due to the rapid developments in the financial services sector due to Fintech, Didenko proposes that Regulators do develop and amend existing regulatory frameworks in order to exercise domestic control and oversight over FinTech.[90]

Chris Brummer and Yesha Yadav in '*Fintech and the Innovation Trilemma'* suggest that if regulation of the financial sector prioritizes market safety and clear rulemaking, then it can be done so through widespread prohibition which will result in the inhibition of financial inhibition. They further argue that in the alternative, if regulators seek to foster innovation while still ensuring that the rights of consumers is observed and respected.

Manuela Geranio in "*Fintech in the Exchange Industry Potential for Disruption*?" correctly asserts that it is a general expectation that Fintech will have a disruptive impact on the financial intermediation sector, thus making finance economical, profitable, convenient for consumers and easy to understand.[91] These would include sectors such as banking, payment services, insurance, and asset management together with stock exchange. Geranio notes that advancement in Fintech has drawn interest from prospective movers and shakers in the technological field (i.e. Google, Amazon, Apple) in addition to key players within the telecommunication industry which in her opinion, would achieve the needs normally had been satisfied by banks and other financial entities.[92] She further notes how conventional players within the financial sector had little option but to make huge investments and commence on new ventures in order to evaluate the probability

[89] Didenko A, 'Regulating FinTech: Lessons from Africa', 19 *San Diego International Law Journa*l, 2017, 311.
[90] Didenko A, 'Regulating FinTech: Lessons from Africa' 311.
[91] Geranio M, 'Fintech in the Exchange Industry: Potential for Disruption Symposium Issue: The British Academy and the Ministry of Science and Technology of Taiwan Project Titled Creating a Legal and Regulatory Framework for Interconnections between Stock Exchanges: A Comparative Study of the UK and Taiwan' 11 *Masaryk University Journal of Law and Technology*, 2017, 245.
[92] Geranio M, 'Fintech in the Exchange Industry', 245.

of disruption caused by Fintech within the financial sector and for the traditional conventional players to be able to safeguard the operations of their business from incoming competitors.

When it comes to stock exchanges which Geranio focuses on, Fintech innovation is highly anticipated to change the course from the implementation and realization of the distributed ledger technology or blockchain to run market infrastructures in a more widely distributed and transparent manner. Thus, as a means of protecting their investments from potential competitors who are in the Fintech industry, there have been proactive changes in exploring blockchain with startups being created to investigate technology.[93]

Finally, Geranio notes that various regulators and international organizations have taken note of in addition to the competition enriching ability of Fintech, but also the varying exposure to virtual threats perhaps related or linked to the distributed ledger technology as new technology provides an avenue for a more open and common accountancy of assets, while removing and eradicating threats related to the single ledger methodology which is widely used nowadays.[94]

Viktoria Chatzara in '*FinTech, InsurTech and the Regulators'* equally takes a similar position that there have been rapid developments in Fintech which have affected the processes and actions within the insurance sector, in addition to also being very disruptive to the processes and actions of the highly capable regulatory agencies.[95] This is because as Fintech keeps on evolving, it reaches a broad range of systems and devices of product delivery and circulation, new ways of fostering of collaboration and assistance among industry players, and furthermore the entrance of non-financial entities into the financial markets, within a worldwide and technologically shaped

[93]Geranio M, 'Fintech in the Exchange Industry', 245.
[94]Geranio M, 'Fintech in the Exchange Industry', 245.
[95] Chatzara V, 'FinTech, InsurTech, and the regulators'4

environment which results in numerous complex circumstances to authorities whenever they exercise their regulatory proficiencies and influence.[96]

In respect to dealing with the regulation of Fintech, Chatzara raises numerous questions which touch on the regulation of Fintech especially questions on which authority would have the capacity to preside over the insurance, banking or investment activities and how much would that regulator preside over those particular industries.[97] Additionally, Chatzara deals with the question concerning the issuance of contradictory decisions by the Regulators. The means and methodology used in regulation of Fintech developments must therefore be critical as most regulators seems to be steps behind the market. [98] Thus, the constant advancement of Fintech has posed a question as to whether the conventional regulatory competences and powers are sufficient for the authorities to properly and adequately implement their institutional responsibilities and duties.

In order to solve the regulatory challenges facing regulators, Chatzara proposes that, for there to be sufficient market supervision, an authority needs to obtain all essential and suitable data in relation to its operations and its participants. Chatzara therefore suggests that regulators do unearth different processes and techniques, to attain suitable and enough data in respect to Fintech applications together with its operations within the financial industry through "RegTech".[99]

Lenore Palladino writes on regulation of Fintech in small business lending in her article '*Small Business Fintech Lending: The Need for Comprehensive Regulation'*. She notes that Fintech lenders have been growing exponentially over the last decade and partly funding small businesses.

[96]Chatzara V, 'FinTech, InsurTech, and the regulators' 4
[97] Chatzara V, 'FinTech, InsurTech, and the regulators'4
[98] Ben Shenglin, Fintech – Challenges to financial regulation and stability, Part of the IFF China Report 2018, available at: https://www.centralbanking.com/central-banks/economics/3456571/fintech-challenges-to-financial-regulation-and-stability accessed on 3 July 2020.
[99] Chatzara V, 'FinTech, InsurTech, and the regulators' 7.

However, small business owners lack the financial skill and know-how in addition to and professional support in dealing with a complex analysis of their loaning options.[100] It is for this reason that Palladino argues that it is crucial for state regulators to maintain an exercise of power over Fintech lenders with a need for amendment of consumer protection statutes.[101]

Joy Malala in Consumer Law and Policy in Kenya,[102] notes that significant steps have been made in Kenya with the enactment of the Consumer Protection Act which gives effect to Article 46 of the Constitution of Kenya, 2010. Malala notes that despite the enactment of a new Act, there are still significant deficiencies particularly touching on which institutions will be tasked with enforcing consumer laws with a gap in certain industries such as the Fintech industry.

Mugo and Kilonzo[103] note that there is a direct link between financial inclusion, reduction of poverty and sustainable growth which can only be delivered if the same are brought within the ambit of mainstream economic activity which also takes into consideration data privacy. Thus, through the protection of consumer data, financial inclusion will permit capital accumulation and asset building which in turn enables persons to reduce their vulnerabilities to poverty.

Barnabas Andiva[104] takes a look into concerns surrounding mobile financial services such as M-Pesa and provides recommendations on how to reduce the exposure of consumers. Andiva acknowledges that mobile commerce transactions and other electronic commerce is a highly evolving arena due the rapid technological advancement and thus there is a huge risk that sufficient

[100] Palladino L, 'Small Business Fintech Lending: The Need for Comprehensive Regulation', 24 Fordham *Journal of Corporate and Financial Law*, 2018, 79.
[101] Palladino L, 'Small Business Fintech Lending', 29
[102] Malala J, 'Consumer Law and Policy in Kenya' *41 Journal of Consumer Policy*, 2018, 356
[103] Mugo M and Kilonzo E, Community-level impact of financial inclusion in Kenya with particular focus on poverty, eradication and employment creation, 2.
[104] Barnabas Andiva, 'Mobile Financial Services and Regulation in Kenya' *Competition Authority of Kenya* (2014)

regulatory responses may not be put in place. This has the effect of questioning whether Regulators indeed have the technical ability and competence to regulate effectively. Andiva thus sets out the existing mobile money services industry in Kenya and offers solutions geared towards mitigating the challenges faced in this sector.

Kinuthia and Akinnusi[105] identify a wide range of factors which were deemed to inhibit the adoption of mobile money services and electronic commerce in Kenya. These include: a lack of resources as well as a constant evolution of technology in the absence of a sufficient regulatory framework. The two authors further observe that electronic commerce has brought forth new risks which ought to be addressed such as internet security concerns, customer and legal related issues including the protection of data. The authors conclude by placing emphasis on the role to be played by the State in guaranteeing a secure environment for electronic commerce. This can be done through the enactment of comprehensive data protection and consumer protection laws, rules and regulations as well as providing sufficient and relevant technical training upon regulators in order for them to be able to sufficiently enforce the enacted legislation.

Aloo[106] studies the regulatory framework surrounding mobile money transactions and other electronic commerce alternatives in Kenya. This was a study was however conducted before the enactment of the National Payment Systems Act and his arguments are thus solely based on advocating for the enactment of a regulatory framework and thus bring to an end the uncertainty.

The Hon. Justice John Mativo, in ***Kenya Human Rights Commission versus the Communication Authority***[107] detailing the dangers of breach of privacy. He stated thus: *"…the processing of*

[105] Kinuthia and Akinnusi, '*The Magnitude of Barriers facing eCommerce Businesses in Kenya'* (2009).
[106] Aloo L.O. 'Mobile Banking in Kenya, Recent Developments – A legal practitioner's perspective' paper presented at UNICITRAL International Colloqium on Microfinance, Vienna, (2011).
[107] Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others [2018] eKLR.

information by the data user/responsible party threatens the personality in two ways: a) First, the compilation and distribution of personal information creates a direct threat to the individual's privacy; and (b) second, the acquisition and disclosure of false or misleading information may lead to an infringement of his identity."

In this research, there will also be an application of various legislations including: the Competition Act, the Consumer Protection Act, the Central Bank of Kenya Act, the Banking Act, the National Payment Systems Act, the Kenya Information and Communications Act, the Capital Markets Act and the Competition Act in addition to the regulations made thereto in those Acts of Parliament as well as various guidelines issued by regulatory authorities. The purpose of reviewing the above legislation would be to identify the shortcomings within the said legislation in respect to the protection of consumer data.

1.10 Limitation of the Study

Taking into consideration the nature of this research, and the novelty of the Fintech industry, the existing regulatory framework is not exhaustive given that regulations of Fintech is still being explored by various regulatory authorities around the world. Indeed, few regulatory authorities have taken significant steps in the integration and regulation of Fintech within the financial system as many have taken the stance of observing from the sidelines on how other states handle the situation before taking any elaborate measures.

This project is further limited to the information accessible to the author and that there is a possibility of certain invaluable information that information which may not be within the reach of the author. Equally, a research of this nature which will most likely have an effect on people's lives requires time to interact with the public in order to determine their nuances, which is well beyond the scope of this research.

1.11 Assumptions

It is assumed that fast paced innovation of technology has resulted in faster integration of technology within financial services and products at a rate that is faster than any reasonable amendment of legislation can be done. It is assumed that this lack of regulation has resulted in inadequate protection of consumers.

1.12 Chapter Breakdown

1.12.1 Chapter 1

This Chapter introduces the topic of the study. It gives the background to the research questions as well as the objectives thereto. Furthermore, this Chapter provides the theoretical and conceptual framework upon which the research will be based and provides views of various scholars in the literature review. Additionally, this Chapter elaborates the methodology, ethical considerations and limitations of the study.

1.12.2 Chapter 2

The second chapter focuses on the concept of fiduciary duties which are placed upon Fintech service providers as information fiduciaries. This involves defining who an information fiduciary is in Fintech transactions and outlines practices may be put in place by the Fintech service providers in conformity with certain fiduciary duties and practices. This Chapter finally sets out the four principle means by which Fintech service providers as information fiduciaries, breach their fiduciary duties towards their customers.

1.12.3 Chapter 3

This Chapter delves into the main research question analyzing the gap within the current legal framework in the regulation of Fintech and Consumer Protection. In doing so, this Chapter

analyses the history of data protection in the digital era in Kenya. This Chapter also looks at decided case law within the Kenya legal system and highlights a variety of sources and guidelines issued by the relevant authorities towards the protection of consumer data in Fintech transactions.

1.12.4 Chapter 4

This Chapter looks at a case study of how consumer data is protected within Fintech entities in other jurisdictions such as the United Kingdom. This is done by focusing on how the concept of privacy in the Fintech arena in the United Kingdom is multi-faceted. This Chapter also analyzes the principles brought forth by the General Data Protection Regulation (GDPR) in respect to protection of consumer data in Fintech transactions. Finally, this Chapter analyzes the applicability of the GDPR in Fintech transactions post-Brexit.

1.12.5 Chapter 5

Chapter Five discusses the findings of the various research questions that will be done as outlined above in the methodology section. These findings are the conclusions of the study. This Chapter equally looks at recommendations and the way forward. The recommendations focus on measures that can be used in Kenya to guarantee the protection of consumer data in Fintech transactions.

Chapter Two: Fintech Service Providers as Fiduciaries

2.1 Introduction

Enacted in 2012, the Consumer Protection Act seeks to bring into force the provisions of Article 46 of the Constitution of Kenya. Despite the enactment of the said provision, there are still fundamental deficiencies in the institutional arrangements under the Act, for instance, on agencies which are tasked with enforcing consumer laws.[108] This is despite consumer protection being considered to be an integral part of regulation within the financial service markets including the Fintech arena. It is important that the consumers of Fintech products are safeguarded from abusive practices including those which may result in their personal data being accessed by third parties without the prior approval of the consumer.[109]

The Constitution of Kenya provides that the Bill of rights applies to all persons, both legal and natural persons who owe obligations to one another.[110] This also includes financial institutions and Fintech companies which do not offer traditional banking services but nonetheless offer access to financial services through the utilization of technology.

Article 31(c) of the Constitution tends to provide two critical aspects of the right to privacy which includes the right to information privacy in respect of one's personal affairs and the right not have information regarding these personal affairs to be revealed without cause. An in-depth analysis of this provision of the Constitution establishes that the right to privacy is thus a right which can be limited through legislation and use of the least restrictive means.[111] This Chapter of this study will

[108] Malala J, 'Consumer Law and Policy in Kenya' *41 Journal of Consumer Policy,* 2018
[109] Good practices for financial consumer protection, The World Bank financial inclusion practice, 2012, 2.
[110] Article 20(1), Constitution of Kenya, 2010
[111] Article 24, Constitution of Kenya, 2010

therefore delve into analyzing Fintech service providers as fiduciaries while also analyzing the existing legal framework governing the protection of data in Fintech transactions.

There is a growing conception that views Fintech service providers as "*information fiduciaries*" which is further seen as a means of balancing freedom of speech with data privacy while still ceding ground for the Fintech service providers to grow.[112] Thus, having taken up the function of designated information fiduciaries, Fintech service providers would have "*special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell and distribute*."[113] Due to the fact that the Fintech service providers are entrusted with sensitive consumer data, it is imperative that it is set out that these Fintech service providers indeed take on fiduciary responsibilities. Indeed, there is a general fiduciary duty imposed on the Fintech service providers who gather or utilize consumer data thus the need for increased regulation of data collection and usage by the Fintech service providers.[114]

It has been argued that the Fintech service providers breach their fiduciary duty when they abuse their consumer's data by utilizing their information to manipulate or discriminate against them, sharing that information with third parties without prior consumer data and violating the privacy policies already put in place by the Fintech service provider.

There is no standard definition of a fiduciary. In ***First Bank of Wakeenye v Moden***[115], a fiduciary has been described as "*The acting of one person for another; the having and the exercising of influence over one person by another; reposing of confidence by one person in another; the*

[112] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations,' *Berkeley Technology Journal* (2018) 4
[113] Jack M. Balkin 'Information Fiduciaries and the First Amendment, 29 *University of California at Davis Law Review*, (2016) 1186.
[114] Jack M. Balkin 'Information Fiduciaries and the First Amendment, 1186.
[115] 235 Kan. 260 (1984)

dominance of one person by another; the inequality of the parties; and the dependence of one person upon another. In addition, courts have considered….knowledge of the facts involved or other conditions giving to one an advantage over the other."

The American Bar Association equally defines a fiduciary to be "*whenever one party places trust and confidence in a second person with that second person's knowledge it is possible that a fiduciary relationship is created*." Thus, fiduciary law has an assumption that service providers and consumers are not necessarily equal. As a consequence thereof, Fintech service providers have a legal obligations to act in the best interests of their consumers for the reason that their consumers entirely on the Fintech service providers.[116] These Fintech service providers who gather and use consumer data are fiduciaries in their services as they are entrusted with sensitive consumer information.[117] These consumers are vulnerable to these Fintech service providers but nonetheless depend on the same Fintech services providers. Equally, the Fintech service providers are deemed to have unrivalled expertise in data collection and use of the collected data. As a consequence thereof, these Fintech service providers have unique responsibilities which require them to act in a manner that preserve the interests of the consumer data which is collected, analyzed, used, sold and possibly distributed.[118]

This has tremendous consequences. Due to the imposition of trust by the consumers upon the Fintech service providers with their information, it is anticipated that the law ought to impose an obligation upon the Fintech service providers to protect the consumers. However, determining that the Fintech service providers owe a '*fiduciary duty'* is insufficient. It is expected that that duty is

[116] Kutcher R. Breach of Fiduciary Duties, in Business Torts Litigation.
[117] Jack M. Balkin 'Information Fiduciaries and the First Amendment,' 1186.
[118] Jack M. Balkin 'Information Fiduciaries and the First Amendment, 1186.

further explained: which practices may be put in place by the Fintech service providers which would be in conformity with their duties and which practices should they avoid?[119]

The trust the consumers place upon the Fintech service providers implies an expectation of predictability.[120] The consumers entrust the Fintech service providers with their data and there is great danger that that trust may be broken when those Fintech service providers utilize that data in a manner that was not initially contemplated by the consumers.

Most of the time, the trust placed upon the Fintech service providers by the consumers exceeds the knowledge of the Consumer of what exactly the Fintech service provider engages in.[121] This has the inevitable result of the consumers misplacing their trust on the Fintech service provider and this has unforeseen consequences.

2.2 Breaching Fiduciary Duties by a Fintech Service Provider

As has already been indicated above, a Fintech service provider can breach its fiduciary duty through four principal means being: manipulation, discrimination, sharing the data with third parties and violating a company's own privacy policy.[122] Where the consumer entrusts a Fintech service provider with their data, the Fintech service provider becomes an information fiduciary which ought to act as such due to the fact failure to do so would result in a breach of the fiduciary duty with serious legal consequences.

[119] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations,' *Berkeley Technology Journal* (2018) 11.
[120] Robert C. Solomon & Fernando Flores, Building Trust: In Business, Politics, Relations and Life (2001) 71.
[121] Robert C. Solomon & Fernando Flores, Building Trust: In Business, Politics, Relations and Life (2001) 71.
[122] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations. Berkeley Technology Journal (2018) 17

2.2.1 Non-Manipulation of the User

The first principle of the fiduciary duty revolves around manipulation: when a Fintech service provider uses information about its consumers to employ underhand tactics which may manipulate them, then this may be deemed to be a breach of the fiduciary duty. More often than not, the consumer may not easily be aware of such breach. Manipulation within the Fintech arena mainly occurs in two ways: where there is failure to respect the autonomy of the customer and thus confront their dignity or where the welfare and interests of the Fintech service provider are placed above those of the consumer. Manipulation would therefore be an attempt to override another person's capacity for reflection and deliberation.[123]

Under the Kenyan Data Protection Act, in order to prevent any manipulation of a consumer based on the data collected by that consumer, there is an obligation imposed upon Fintech service providers to ensure that the personal data of consumers that is collected is processed in a lawful manner which is also fair and transparent in relation to the consumer.[124]

2.2.2 Antidiscrimination

This is the second principle that Fintech service providers, who act as information fiduciaries, are expected to follow. It involves not discriminating between or against its consumers based on certain characteristics, which could include race or gender. There are three main means by which the Fintech service provider may discriminate against a consumer based on the certain characteristics. These include through access to services, prices of their services and digital redlining.[125]

[123] Cass R. Sunstein, Fifty Shades of Manipulation 1 *Journal of Behaviour* (2015), 239.
[124] The Data Protection Act, s. 25.
[125] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations' *Berkeley Technology Journal* (2018) 25.

In its duty as a fiduciary, a Fintech service provider ought not to offer varying services or prices to individual customers simply based on their membership or non-membership in a protected class. It is normally not the expectation of Consumers that when they hand over their data through various technological platforms, that they are making it easier for the Fintech service providers to use that same data to discriminate against them. Given that the said users do not anticipate this, they therefore cannot take reasonable measures to prevent their own data from being used against them by selecting service providers in a more carefully manner or electing not to provide certain information concerning them.[126]

Fintech service providers can easily triangulate to ascertain a consumer's preferences and dislikes and the consumer is highly unlikely to anticipate this or hide certain information concerning them.

One way in which the Fintech service provider could discriminate against the consumers is through offering different services to different consumers. This service discrimination is not easily discernible to the consumer when they engage in a normal online transaction. Looking at it from a different angle, these tailored services are mostly seen as a feature of Big Data instead of a bug.

Data collection is further viewed as making price discrimination easy. Thus, a Fintech service provider may quite easily identify which consumer is more likely to pay higher prices or at which specific periods are they more likely to do so and then adjust the price of a certain Fintech service based on that data.

In addition to above, while it is has not been clearly established whether many Fintech service providers do actually offer different services or prices based on membership in a protected class, the Fintech service providers can discriminate through zip code, which can be seen to be a proxy

[126] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations,' 17.

for membership in a protected class. Even though this is now illegal, these practices, commonly referred to as redlining,[127] has been an enabler of discrimination. In a similar manner, internet protocol addresses can be likened to zip codes, which tend to permit most firms to be able to determine the location of their consumers when they access certain technological applications.

In the Kenyan context, in order to prevent the discrimination of the consumers of Fintech services, the Data Protection Act not only places an obligation upon the Fintech service provider to process consumer data in a lawful, fair and transparent manner, but also places an obligation upon the Fintech service provider to collect, for explicit, specified and legitimate purposes that consumer data which is not to be further processed in a manner that would be incompatible with the intended specific and legitimate purposes.[128]

2.2.3 Limited Sharing With Third Parties

This is a major concern for Fintech firms which act as fiduciary of persons' data as they face the question: to whom can we disclose a consumer's data to? Most Fintech Service providers have in place privacy policies which govern how they are able to choose third parties with whom they share user information. However, in certain circumstances, the sharing of the personal data results in a violation of the fiduciary duty as that personal data is often given in confidence, with the expectation that it would not be shared with anyone else apart from the Fintech service provider.[129]

In the consideration of a fiduciary duty for Fintech service providers, it is essential to be able to decide with which third parties the consumer data can be shared with in a manner that still meets the Consumer's expectations at the time of providing the data to the Fintech service provider. In

[127] Redlining is "the illegal practice of refusing to offer credit or insurance in a particular community on a discriminatory basis. MERRIAM–WEBSTER, https://www.merriam-webster.com/legal/redlining [http://perma.cc/6BFU-6469] accessed on 3rd May 2021

[128] Data Protection Act, s 25(c)

[129] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations,' 17

nearly all circumstances, a third party which receives data from a Fintech service provider automatically includes an information fiduciary to the consumer and is thus expected to adhere to all the responsibilities allocated to the original fiduciary. It is therefore imperative that Fintech service providers should not share data with entities that do not uphold information fiduciary duty as doing so knowingly will also be a violation of the Fintech service provider's own duty as well.[130]

Under the Kenyan legal system, in order to limiting of consumer data with third parties, there is an obligation placed upon Fintech service providers to ensure that the consumer data they collect in Fintech transactions is adequate, relevant and limited to what is necessary in relation to the purposes for which the said information is to be processed.[131]

2.2.3 Violating the Company's own privacy policy

This final principle prohibits Fintech firms from violating their own privacy policies. A Fintech service provider, as an information fiduciary is thus expected to comply with the restrictions it imposes upon itself.

2.3 Conclusion

From the above, it is evident that Fintech service providers are to be held to an information fiduciary standard as one of the means which will guarantee data-focused business models can continue to operate while the consumers remain to be adequately protected. The four principles outlined within this chapter – anti-manipulation, antidiscrimination, limited third party sharing and holding companies to their own privacy policies – are all geared towards safeguarding consumer expectation. These four principles as has been demonstrated within this Chapter are also provided for under sections 25(b), (c) and (d) of the Data Protection Act.[132] With the constant evolution of

[130] Dobkin A. 'Information Fiduciaries in Practice: Data Privacy and User Expectations,' 17.
[131] Section 25(d), Data Protection Act.
[132] Act No. 24 of 2019

technology, the expectation of the consumers may change. Despite this shifting expectation, there ought to be a complete safeguard of privacy standards by these entities.

Chapter Three: The Development of Kenya's Legal and Regulatory Framework for Data Protection in Fintech Transactions

3.1 Introduction

Technological innovation has taken the driver's seat in the development in Kenya particularly through the use of mobile money and other retail financial services.[133] For instance, the use of mobile money has revolutionized the manner in which financial services are being rendered in Kenya by bringing a large number of "*unbanked*" and "*under-banked*"[134]

In the present technological era, discussions as to privacy have been brought to a whole new level given a deeper understanding of the meaning and cost of privacy.[135] Before delving into the importance of consumer privacy within the Fintech arena, it is paramount that the concept of privacy is elaborated on. The Universal Declaration of Human rights expressly provides that "*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, not to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[136]

Kenya has enacted electronic transactions legislation.[137] It had however, initially been argued that the said legislation was not sufficient for the needs of all commercial operators, including the needs of mobile payment providers. For instance, in 2011, Kenya enacted the National Payment System

---

[133] Malala J, Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it presents for mobile payments, WPS/02/14 KBA Centre for research on financial markets and policy working paper series.

[134] The 'unbanked' and the 'under banked' will be used in this paper to refer to persons who do not hold bank accounts or who rely on alternative financial services. See "Tapping the Unbanked Market" Symposium". Federal Deposit Insurance Corporation (FDIC) <http://www.fdic.gov/news/conferences/TUM_bio.html> accessed 3rd May 2021.

[135] Serban Andrea, ' the Value of privacy: what does the Personal Data Mean to the Data Subject and Businesses? *Current Issues in Business Law Journal* 2018.

[136] Article 12, the Universal Declaration of Human Rights, United Nations General Assembly resolution 217 A, 10th December 1948 available on https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks. Accessed on

[137] Malala J, Consumer Protection for Mobile Payments in Kenya.

Act, a regulatory framework which explicitly allowed the use of electronic means as a method of providing payment services. This Act did not however set out the rights expected in respect to data protection in electronic financial services. Thus, the consumer protection regime for payment systems in Kenya in respect to data protection remained to be fragmented.[138] Despite this however, the National Payment System Department within the Central Bank of Kenya provides oversight to mobile payments on the integrity of the information technology and service delivery systems. This is however focused on protecting consumers from "operational failures."

Prior to the enactment of the Consumer Protection Act 2012, consumer protection in Kenya lacked a comprehensive framework.[139] The Banking Act gave authority to the Central Bank of Kenya to regulate banking activities but failed to define the specific mandate for protection of consumer data collected by financial institutions. Before an analysis of the above is delved into, it is imperative to set out the history of data protection in the digital era in Kenya.

3.2 History of Data Protection in The Digital Era in Kenya

3.2.1 Pre-Independence Era

The issue of privacy in Kenya can be traceable to the colonial era. The colonial master had in place a Native Registration Ordinance in 1915 which served to introduce the "*Kipande System*" that registered a fingerprint of the applicant. This Registration Ordinance was amended in 1949 to pave way for the issuance of national identity cards and was not elaborate on the protection of data of the holders of the said cards.

[138] Malala J, Consumer Protection for Mobile Payments in Kenya
[139] Malala J, Consumer Protection for Mobile Payments in Kenya

3.2.2 Post-Independence (1963-2010)

The Independence Constitution set out an elaborate Bill of Rights that was more or less similar to the contents of the European Convention on Human Rights.[140] Indeed, that Constitution granted every person the freedom to "*hold information as well as receive ideas and information without interference from the state or any agencies*."[141] This right however, was not absolute but could be limited on grounds of national security, safety and public health.[142] With the advancement of computers and information technology at the turn of the 20th Century, the Kenya Information and Communications Act[143] was enacted. This Act provided to be a major turning point in respect of data protection as it enabled the timely and effective detection, prohibition, prevention, response and prosecution of computer and cybercrimes.

3.2.3 Post-2010

The Constitution of Kenya, 2010, is the supreme law of Kenya and is binding upon all persons and state organs both at the national level of government and the county level of government.[144] The validity of the Constitution of Kenya is absolute and the provisions contained within the Constitution cannot be challenged before any court of law or state organ.[145] The sovereign power of the people of Kenya is exercised through the Constitution as provided under Article 1 of the said Constitution. Therefore, being the supreme law of Kenya, it is required that all written laws be consistent with the provisions of the constitution.[146] These written laws include the statutes governing Fintech transactions and the protection of privacy within these transactions.

---

[140] Sarah Nyakio "Digital rights; the Present and the Future", ICJ-Kenya, https://www.icj-kenya.org (Accessed 24 April 2020).
[141] Section 79(1) of the repealed Constitution.
[142] Section 79(2) of the repealed Constitution.
[143] Act No. 2 of 2018
[144] Article 2(1), Constitution of Kenya, 2010.
[145] Article 2(3), Constitution of Kenya, 2010.
[146] Article 2(4), Constitution of Kenya, 2010.

The Constitution has been praised globally as being one of the most progressive and liberal regimes of human rights protection with provisions within the Bill of Rights therein, containing the right to privacy and the right to access to information, which rights must be respected, protected, fulfilled, observed and promoted by all organs and agencies of government as well as individuals. Article 10 of the said Constitution also provides for the national values and principles of governance which include among others the rule of law, democracy, participation of the people, integrity, transparency and accountability. All these are essential in the implementation of data rights in financial transactions as the values under the provision relate to privacy and data protection as part of human dignity and human rights. Human dignity has been established as the foundation of the right to privacy.[147]

As a fundamental right, the right to privacy is highly protected and promoted among other fundamental rights and freedoms. Chapter Four of the Constitution provides for the Bill of Rights.[148] Under Article 21, every person and all state organs have a duty to observe, respect, protect, promote and fulfil the rights and fundamental freedoms in the Bill of Rights.[149] The State is further obligated to enact and implement legislation to fulfil its international obligations in respect of human rights and fundamental freedoms.[150] Given that human rights are interventions of justice and reason to provide protection, there is a need to have the said rights observed and

[147] Florida L. On Human Dignity as a Foundation for the Right to Privacy, *Philosophy & Technology Journal* (2016), 307.

[148] Chapter 4 is divided into five parts. Part 1 sets out the general provisions relating to the Bill of Rights. Part 2 sets out the actual rights and fundamental freedoms. Part 3 sets out specific application of rights by elaborating on certain rights to guarantee greater certainty as to the application of those rights and fundamental freedoms to certain groups of persons, though this part is not to be interpreted as limiting or qualifying any right. Part 4 sets out the applicability of rights and fundamental freedoms where a state of emergency has been declared and in what circumstances can a state of emergency be declared as well as the legality of a state of emergency. Finally, Part 5 establishes the Kenya National Human Rights and Equality Commission which performs various functions in order to promote the respect for human rights and develop a culture of human rights in Kenya.

[149] Article 21(1), Constitution of Kenya, 2010.

[150] Article 21(4), Constitution of Kenya, 2010.

promoted in order to guarantee that human dignity is upheld and to further promote social justice and realize the human potential as required under Article 19(2).[151] The Bill of Rights is therefore an essential component of Kenya as a democratic state.[152]

Equally, the Constitution of Kenya, 2010 under Article 31 recognizes the right to privacy.[153] This Article provides for four aspects in respect to the right to privacy. The first one is that a person is not to be arbitrary searched, which extends upon a person and his property to ensure that authorities and any other person, including Fintech service providers do not interfere with one's private life, including, but not limited to family.[154] This right is applicable to both individual Fintech consumers as well as corporate Fintech consumers. The second aspect of the protection under Article 31 is the protection from seizure of possessions which also affects the right to property and seeks to protect individuals from the state that can deprive the citizens off their property.[155]

The third aspect of the right to privacy under Article 31 seeks to prevent information concerning a Fintech consumer's family from being unnecessarily revealed or required. It is mostly under this limb of the right to privacy that data protection applies. This right is therefore constantly developing pursuant to the right to privacy.[156] The right to data protection, under Article 31 of the Constitution, is therefore a constitutive or a derivative right of the right to privacy.

---

[151] Frankenberg G. Human Rights and the Belief in a Just World, 12 *Oxford University Journal* (2014), 37.
[152] Article 19, Constitution of Kenya, 2010.
[153] Article 31 provides that 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.
[154] Emberland M. Protection against unwarranted searches and seizures of corporate premises under Article 8 of the European Convention on Human Rights; the Colas Est SA vs. France Approach, 84.
[155] Alvarez J. The Human Right to Property, *University of Miami Law Review*, 587.
[156] LA Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, 6 International Journal of Law and Information Technology* (1998), 254.

The fourth and final aspect contained under Article 31 of the Constitution which is also related to data protection but heavily touches on Fintech transactions as it protects the privacy of one's communications. Communications, especially in the era of technology, covers a large spectrum including electronic transactions. The interception of communication within Fintech transactions by the state, non-state actors and other third parties within Fintech transactions has been a serious infringement of privacy.[157] This aspect as contained under Article 31 has therefore called for enactment of legal steps aimed towards safeguarding communication within Fintech transactions, thus, placing a greater responsibility upon Fintech service providers. This is especially so through the imposition of liability upon Fintech service providers.[158]

As has already been indicated above, in order to guarantee that human rights are protected, the State is obligated to Act as the duty bearer in the protection human rights. These human rights can only be fulfilled in situations where their correlative duties are performed. Similarly, human rights are abused where there is non-performance of those correlative duties.[159] The Constitution further provides that the state has the mandate to guarantee the enjoyment of rights in such a manner that the said enjoyment of rights does not affect the enjoyment of the rights of others. Thus, the state has an obligation to protect, observe, promote, respect and fulfil the fundamental rights provided in the Constitution.[160] The state therefore bears the greatest responsibility in the promotion of data protection and privacy in Fintech transactions.

[157] Kierkegaard S. Privacy in Electronic Communication: Watch your Email, your boss is snooping. 21 Computer Law & Security Review (2005), 228.
[158] Simitis S. Privacy – an Endless Debate? *California Law Review* (2010), 1992.
[159] Mavriocola N. What is an Absolute Right? Deciphering Absoluteness in the Context of Article 3 of the European Convention on Human Rights, *12 Human Rights Law Review*, 729 (2012).
[160] Article 21, Constitution of Kenya, 2010

The Constitution also requires the state to enact and implement legislation to enable it fulfil its international obligations in respect of human rights and fundamental freedom. In situations where the state fails or is unable to fulfil its international obligations, Article 22 of the Constitution provides for enforcement of human rights, including the right to privacy under Article 31 of the Constitution, through Article 22 of the Constitution. This enforcement is conducted through proceedings filed in Court.[161] The enforcement proceedings, touching on infringement of Article 31 of the Constitution may be instituted by a person acting on behalf of another person who cannot act in their own name; a person acting as a member of, or in the interest of, a group or class of persons; a person acting in the public interest; or an association acting in the interest of one or more of its members.[162]

The jurisdiction to hear and determine petitions touching on infringement of human rights is conferred upon the High Court.[163] This is similar to the global practice where courts, particularly in Europe and USA are presently handling cases touching on data protection and the right to privacy.[164] This therefore demonstrates the pivotal role played by the courts in ensuring the protection of consumer data in Fintech transactions.

Article 20 of the Constitution is titled "*Application of Bill of Rights*." This Article places an obligation upon the judicial system to develop the law to the greatest extent possible that it does not give effect to a fundamental freedom. This Article further places an obligation upon the Court

[161] Article 22(1) of the Constitution provides that 'Every person has the right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened.'
[162] Article 22(2), Constitution of Kenya, 2010.
[163] Article 165(3)(b) of the Constitution provides that: 'the High Court shall have jurisdiction to determine the question whether a right or fundamental freedom in the Bill of Rights has been denied, violated, infringed or threatened.'
[164] Some of the recently concluded cases can be found https://inforrm.org/2020/01/06/top-10-privacy-and-data-protection-cases-of-2019-a-selection-suneet-sharma/ accessed on 17th June 2021.

to render interpretations of the law in a manner that most favours the application of rights and fundamental freedoms such as the right to privacy. This is important especially when the courts need to balance the right to privacy in Fintech transactions when that right is competing with other rights.

Consequently, the government has in place the national ICT policy as well as the Data Protection Act which tend to address the major concerns for privacy in the way information is processed. Kenya has equally ratified the International Covenant on Civil and Political Rights 1976, which places emphasis on the enactment of domestic legislation around the principles that touch on the protection of privacy and individual liberties.[165] In addition to the above, Kenya is a party to other conventions such as the African Charter on Human and People's Rights as well as the African Union Convention on Cyber Security and Personal Data Protection (2014). It is therefore evident that consumer protection measures have been put in place, in respect of consumer data privacy by Fintech consumers.

The incorporation of technology in finance has had the net effect of eroding privacy which most people enjoy with the net effect of having a digital footprint capable of being tracked by government and persons, both natural and legal, in unimaginable ways.[166] This is the main premise behind Fintech lending as that industry utilizes technology in credit and customer decision making and majorly set loan prices based on data collected from digital profiles. This enables the Fintech

[165] Article 17 of the International Covenant on Civil and Political Rights provides that "No person shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

[166] Can Digital Footprints Lead to Greater Financial Inclusion? Available on https://www.cgap.org/sites/default/files/CGAP-Brief-Can-Digital-Footprints-Lead-to-Greater-Financial-Inclusion-Jul-2012.pdf

service providers to be able to quickly determine whether a consumer is a good risk for financial undertakings.[167]

This digital footprint, in Kenya, is constantly growing as Fintech lenders are constantly collecting data from their sites as well as information collected from public websites. This is equally applicable to mobile money transfers in Kenya through M-Pesa, with this data being available to entities and posing a threat to various rights.

MPESA, is a mobile banking service within Kenya that permits users to store and transfer money through their mobile phones.[168] The introduction of M-Pesa in Kenya was to provide an alternative means for the Country's population to have easy access to financial services. MPESA has resulted in financial inclusion for a large portion of the Kenyan population which is unbanked as it is able to deliver low-cost financial services to the unbanked and underserved.[169] MPESA is therefore used to transact high volumes of financial transactions within large segments of the population making it an integral part of the financial system for consumer. There is therefore a great need to protect consumer interests and ensure the implementation of policies to manage operational risk, safeguard and ring-fence customer money as well as data, while planning for business continuity.[170]

The Central Bank of Kenya Act at **section 4A (d)** grants the Central Bank of Kenya (CBK) the absolute discretion to "*formulate and implement such policies as to best promote the*

[167] Fintech lenders are tracking and judging your digital trail. Available on https://www.inquirer.com/philly/blogs/inq-phillydeals/fintech-data-mobile-online-social-media-search-tracking-digital-footprint-joseph-n-distefano-20180703.html
[168] https://www.investopedia.com/terms/m/mpesa.asp
[169] Muthiora B, Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Money for the Unbanked, *Bill & Melinda Gates Foundation*, 2015, 7.
[170] Muthiora B, Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Money for the Unbanked, 7.

establishment, regulation and supervision of efficient and effective payment, clearance and payment systems." This Act was however insufficient of the statutory role to be performed by the CBK regarding regulations touching on payment services that were to be rolled out by the CBK. This statutory authority was later on granted vide the enactment of the National Payment System Act.[171]

In line of the aforementioned requirement, Kenya has recently enacted new legislation but there are little answers as to how data subjects within the Fintech arena perceive the concept of privacy and how data processing affects them under the new statute. This new statute is the Data Protection Act, 2019.

The enactment of the Data Protection Act majorly arose from the right to privacy. This legal framework is deemed to be largely associated with national security, right to information and also cyber security.[172] This is due to the fact that data protection has become an integral element in Fintech transactions especially in the current era of big data in which individuals as well as consumers, seek to have better and enhanced control over their personal data.[173] This desire to have enhanced control over personal data is largely viewed as being synonymous and interchangeable with the right to privacy.[174]

[171] 2012
[172] Lynskey O. 'The Foundations of EU Data Protection Law', *1 Ed. Oxford University Press*, 2015, 2.
[173] Lynskey O. 'The Foundations of EU Data Protection Law', 2.
[174] Makulilo A. Privacy and Data Protection in Africa: A state of the Art,' *2 International Data Privacy Law* (2012) 177.

3.3 An Analysis of The Existing Legislative Framework That Governs Data Protection

3.3.1 The Data Protection Act

The principle legislation that governs data protection in Kenya is the Data Protection Act.[175] The Data Protection Act is an Act of Parliament enacted to give effect to Article 31(c) and (d) of the Constitution.[176] The incorporation of Fintech in finance through the use of Digital lending applications fall within the ambit of the Data protection Act for the reason that they are actively involved in processing of personal data.[177] Furthermore, these Digital Lending Applications have access to different types of data, including but not limited to phone identity, messages on the phone, network connections, phone storage and location of the bearer of the phone.

The Data Protection act has been lauded for setting out principles that persons processing data are expected to follow.[178] The Data Protection Act provides that every person has a right to be protected from unnecessary disclosure of their private and family affairs.[179] The implication of this within the Fintech Arena is that the taking up of loans through digital lending apps ought not to be disclosed to any other person except the borrower.

The Act further requires that the data collected in financial transactions which are assisted by technology are processed in a lawful manner which is equally fair and transparent.[180] This therefore places an obligation upon Fintech firms to disclose the information they collect from the consumers of their products, and how that information is processed. The data collected must

[175] Act No. 24 of 2019
[176] Article 31(c) and (d) provide that every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.
[177] Privacy and Data Protection Practices of Digital Lending Apps in Kenya, 2020, Strathmore University, Center for Intellectual Property and Information Technology Law.
[178] Part IV of the Data Protection Act contains the Principles and Obligations of Personal Data Protection.
[179] Section 25(a), Data Protection Act.
[180] Section 25 (b) Data Protection Act.

therefore be in accordance to either a law or a legitimate purpose, which in the case of Fintech services, could be credit scoring and keeping business records.[181]

Section 25(c) of the Act, in respect to Fintech transactions, requires that Borrowers ought to be given information on the reasons as to why their information is being gathered by the various Fintech firms. Thus, Fintech service providers are precluded from repurposing the data collected without prior knowledge and approval of the borrower.

The Data protection Act also places a limitation upon Fintech service providers to process information that is relevant and sufficient for their purposes.[182] This is because Fintech service providers have access to data which is freely given by borrowers at registration, on top of data that is collected by the various technological applications utilized by the borrowers, together with data which is the product of an analysis of the first two types of data.

Under the Data protection Act, there is an obligation placed upon Fintech Service Providers to ensure that a valid explanation is given when information concerning family or private affairs is to be collected.[183] The reasoning behind this is that Fintech service providers place heavy reliance, while determining creditworthiness, upon results of analysis of phone data and other data collected from devices used by the various Fintech consumers. This grants the Fintech service providers access to personal data on the borrower's family and private affairs, thus the rationale that there ought to be safeguards and explanations as to why family and private information is required.

[181] Privacy and Data Protection Practices of Digital Lending Apps in Kenya, 2020, *Strathmore University, Center for Intellectual Property and Information Technology* Law. Pg.8
[182] Section 25(d) Data Protection Act.
[183] Section 25(e), Data Protection Act.

The Data Protection Act also requires that adequate information should be kept by Fintech Service Providers, which information is constantly updated in order to guarantee that incorrect personal information is immediately remedied or removed.[184] This requirement is in addition to a retention requirement placed which obligates Fintech service providers not to keep data in perpetuity than is necessary for the purposes for which the said data was collected.[185] This, therefore requires Fintech service providers to ensure that the various consumers are notified of how long their data would be kept and the purpose of keeping that data.

Finally, the Data Protection Act prohibits the transfer of Consumer Data by Fintech service providers outside Kenya without evidence of sufficient data protection safeguards on top of the prior approval of the consumer.[186]

3.3.2 Other relevant provisions of the Data Protection Act

In addition to the aforementioned provisions of the Data Protection Act, there are other relevant provisions of the Data Protection Act which are relevant to Fintech companies such as: the rights of data subject, direct collection of data from the data subject, various notification requirements, data protection impact assessment, automated decision making, data portability, and data protection by design and default.

3.3.2.1 Rights of the data subject.

Consumers of Fintech lenders can be termed as data subjects with the right to information of how their information/data will be used.[187] These consumers of Fintech thus have a right to be able to

[184] Section 25(f), Data Protection Act.
[185] Section 25 (g), Data Protection Act.
[186] Section 25(h), Data Protection Act.
[187] Section 26, Data Protection Act.

access their personal data which is held by the Fintech lender and, in some circumstances, raise an objection as to the processing of part of their data by the Fintech lender.

3.3.2.2 Collection of data from the data subject

Section 27 of the Data Protection Act envisages a situation where data is supposed to be collected directly from the data subject/consumer. However, in the case of lending through Fintech firms, it must be noted that most of the data collected are mainly from the consumer's smartphone or other sources.[188] Any other collection done by the Fintech firms is subject to the consent of the data subject. The Data Protection Act defines consent as "*the manifestation of express, unequivocal, free, specific and informed*" agreement by the data subject.[189] Fintech firms are known to collect data through inference, which is a concept not known to consumers.

3.4 Other relevant Kenyan Statutes:

There are other notable Kenyan statutes which govern the activities of Fintech service providers in Kenya particularly where data of the Fintech consumers is involved. These include the following: the Computer Misuse and Cybercrimes Act.[190] This Act provides for cybercrime offences in Kenya. Another relevant statute is the Kenya Information and Communications Act.[191] This statute was enacted in order to enable the development and growth of the information and communications sector as well as electronic commerce. The Kenya Information and Communications (Consumer Protection) Regulations, 2010 which had been enacted to protect the consumer of technological and communication services and products.

[188] Privacy and Data Protection Practices of Digital Lending Apps in Kenya, 2020, Strathmore University.
[189] Section 2, Data Protection Act
[190] Act No. 5 of 2018.
[191] Act No. 2 of 1998

3.4.1 The Computer Misuse and CyberCrimes Act

This is an Act of Parliament that establishes various offences that relate to computer systems. These offences include unauthorized access or interference, cyber espionage, cyber harassment, cybersquatting, phishing and cyber terrorism. This Act also contains provisions that enable the timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes which can be coupled with international cooperation when relating to computer and cybercrime particularly in the Fintech arena.

This Act further allows for information sharing which is however limited between the owners of critical data information. This is further limited to certain information such that the sharing of health status information without the consent of the consumer is not permissible. This is the implementation of a fundamental data protection principle.

The objectives of this Act include the protection of the confidentiality, integrity and availability of computer systems, programs and data; preventing the unlawful use of computer systems; facilitating the prevention, detection, investigation, prosecution and punishment of cybercrimes; protecting the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and facilitating international co-operation on matters covered under the Act.

Unfortunately, and insufficiently, under this Act, the word ‘privacy’ has been merely mentioned as “as an obligation of state agents during investigations to the extent that they have an obligation to take measures in preparation of real-time collection or recording of content data while

maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party that is not part of an investigation.[192]

It must however be noted that certain sections of the Act had been declared as unconstitutional with the Court directing the Attorney General to amend and reenact those sections. These sections include sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52 and 53.[193]

3.4.1 The Kenya Information and Communication Act

Despite this Act being a fairly old Act of Parliament, it was recently amended in 2019 with the effect of the Act now being able to regulate electronic transactions and cyber-security, which are core to the operation of various Fintech service providers. This regulation of electronic transactions and cyber-security is to be done through the Communications Authority of Kenya which is expected to develop a framework to enable the speedy investigation and prosecution of cyber-crime offences involving data and to further facilitate the efficient management of certain important internet resources.

3.4.1 Kenya Information and Communications (Consumer Protection) Regulations

These regulations are enacted pursuant to the Kenya Information and Communications Act. These Regulations specifically set out the rights and obligations of consumers within the Fintech arena while also taking into account the safeguards that licensed telecommunication service providers, such as Safaricom, which participates in Fintech through its M-Pesa platform, ought to put in place to guarantee that the rights of their consumers are adequately protected. These regulations further

[192] Sections 52 and 53, Computer Misuse and Cybercrimes Act
[193] Bloggers Association of Kenya (Bake) v Attorney General & 5 Others [2018] eKLR.

require the various Fintech service providers to take sufficient technical and organizational measures the safeguard the security of their services including consumer data.

3.4.2 The Draft Data Protection (General) Regulations, 2021

Kenya is also further in the process of enacting the Data Protection Regulations.[194] These Regulations essentially give effect to and operationalize the Parent Statute being the Data Protection Act. The Regulations are therefore essential in data protection in Fintech transactions in the following manner:

3.4.1 Requirement of prior consent by the Fintech Consumer

Regulation 4 places an obligation upon a Fintech service provider to inform the consumer of the nature of personal data that will be collected by that Fintech service provider, the scope of the data that will be processed, the reasons for processing the required personal data and whether that data would be shared with other third parties.[195] This information ought to be made accessible to the consumer prior to the collection of the personal data. In obtaining the said prior consent from the Consumer, the Fintech service provider is expected to ensure that the consumer has the capacity to understand and communicate his/her consent, the consumer is informed of the nature of the processing in a simplified and clear manner, the consent is voluntarily issued, free without any threats of coercion and the consent is specific to a particular category of data.[196] This consent may be oral or written but ought not to be implied.

3.4.2 Imposition of restrictions to processing of data

A consumer is entitled to lodge a request with the Fintech service provider to restrict the processing of their personal data, where the consumer feels that the personal data is inaccurate, where the said

[194] These regulations are made pursuant to section 71 of the Data Protection Act.
[195] Regulation 4(1) Data Protection (General) Regulations, 2021.
[196] Regulation 4(3) Data Protection (General) Regulations, 2021.

data has been unlawfully processed, where the consumer no longer needs that personal data but is apprehensive that the data will be required to establish, exercise or defend a legal claim, or where a consumer has lodged an objection to the processing of his/her personal data and the Fintech Service provider responds by issuing legitimate grounds that override those of the consumer.[197]

3.4.3 Rectification of personal data

The Regulations further present an opportunity for consumers of Fintech services to remedy any inaccurate, outdated, incomplete or misleading information that is in the possession of the Fintech service provider.[198] This request for rectification is to be made in a format that is prescribed by the Regulations. Once the request for rectification has been made, the Fintech service provider is under an obligation to rectify the entry of the said data within seven days especially after it is satisfied that the rectification is necessary.[199]

3.4.4 Restriction on the Commercial Use of Personal Data

Part III of the Regulations provide for the restriction on the commercial use of personal data. Thus, a Fintech service provider is only permitted to use the personal data of consumer, with the exemption of sensitive information only if that Fintech service provider has collected the said personal data from the consumer who had been earlier on informed that direct marketing is one of the purposes for which the personal data is collected and that consumer has consented to the use or disclosure of that personal data for that direct marketing purpose for which the consumer may ask not to receive direct marketing communications.[200]

[197] Regulation 6(2) Data Protection (General) Regulations, 2021.
[198] Regulation 9(1) Data Protection (General) Regulations, 2021.
[199] Regulation 9(4) Data Protection (General) Regulations, 2021.
[200] Regulation 14 Data Protection (General) Regulations, 2021.

3.4.5 Obligations of Fintech service providers

The Regulations equally set out the obligations of Fintech service providers as data controllers and data processors.[201] Thus, a Fintech service provider is expected to have a personal data retention schedule which sets out the requisite timelines which take into account the purpose, period and has a provision for periodic audit of data retained and actions to be taken on matters arising out of the said audit.[202] This provision is to be enacted pursuant to section 39 of the Data Protection Act.

The General Regulations further make provision for a data-sharing code which a Fintech service provider can share or exchange personal data which it had collected, following a request from another Fintech service provider.[203] The Draft General Regulations thus provide instances during which data sharing can be permitted which instances include providing personal data to a third party, providing third party with access to personal data on the Fintech service provider's information systems and receiving personal data as joint participants in a data sharing arrangement.

A Fintech service provider is therefore expected to have a Data Protection Policy which is regularly updated and reflects its personal information handling practices.[204] The minimum requirements of such a policy is that it should include: the nature of personal data collected and held, how a consumer may access their personal data and exercise their rights in respect to that personal data, have a complaint handling mechanism. The policy must also state the lawful purpose of processing personal data while setting out obligations or requirements to transfer personal data outside Kenya to third parties outside Kenya.

[201] Part IV Data Protection (General) Regulations, 2021.
[202] Regulation 18, Data Protection (General) Regulations, 2021.
[203] Regulation 20, Data Protection (General) Regulations, 2021.
[204] Regulation 22, Data Protection (General) Regulations, 2021.

3.5 Regional Initiatives on Data Protection

Kenya is equally party to certain regional initiatives which govern the protection of consumer data within Fintech transactions. These regional initiatives in data protection are comprehensive due to the interests which they tend to protect at the regional level. Among the regional initiatives which Kenya is part of include the Convention on Cyber security and Personal Data Protection 2014. This Convention was adopted by the AU Assembly in 2014. Kenya has however neither signed nor ratified the said convention.

3.5.1 The AU Convention on Cyber security and Personal Data Protection (AU Convention)

The principle objective of this Convention is to set the essential rules for creating a credible digital environment while addressing the gaps that affect the regulation and legal recognition of electronic communications and electronic signature; together with the absence of specific legal rules that ought to safeguard consumers, intellectual property rights, personal data and information systems and privacy online.[205] It is a principle aim of this Convention to encourage the enactment and development of national and sub-regional frameworks for cyber security and data protection within the African continent while harmonizing the legislative framework of its member states on various aspects of Fintech transactions, including, but not limited to electronic commerce, data protection, cyber security governance and cybercrime control. It is a requirement under the Convention for State Parties to establish legal frameworks to promote the protection of physical data.

Chapter II of the Convention covers the protection of personal data.[206] These provisions include the level of applicability of the AU Convention with regard to personal data protection and preliminary personal data protection formalities.[207] The provisions of Chapter II of the Convention

[205] Preamble to the African Union Convention on Cyber Security and Personal Data Protection (2014).
[206] Chapter II of the AU Convention on Cyber Security and Personal Data Protection is titled 'Personal Data Protection.'
[207] Section 1 of Chapter II of the AU Convention on Cyber Security and Personal Data Protection.

further provide an institutional framework for the protection of personal data by obligating member states to establish national personal data protection authorities.[208]

Section III of Chapter II of the Convention establishes the basic principles which govern the processing of consumer data in Fintech transactions. These include: the principle of consent and legitimacy of personal data processing; the principle of lawfulness and fairness of personal data processing; the principle of purpose relevance and storage of processed personal data; the principle of accuracy of personal data; the principle of transparency of personal data processing and finally, the principle of confidentiality and security of personal data processing.

It must however be noted that at the time of this study, the Convention has only been signed by fourteen countries with eight having ratified the same.[209] It can therefore be concluded that the said Convention has no discernible impact on data protection standards in Kenya and the region.

3.6 Kenyan Jurisprudence on Data Protection

The Judiciary in Kenya has made bold steps towards protection of privacy in Fintech transactions as has been decided in various cases. This has been done through purposive and broad interpretation of the Constitution. This can be demonstrated in both pre-2010 and post-2010 decisions of the High Court. Before the enactment of the Constitution in 2010 for instance, the Courts held that section 70 of the then Constitution protected the right to privacy with the effect

[208] Section 2 of Chapter II of the AU Convention on Cyber Security and Personal Data Protection. This section is titled Institutional Framework for the protection of personal data, while Article 12 provides for the duties and powers of National Protection Authorities.

[209] List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection, available on https://inforrm.org/2020/01/06/top-10-privacy-and-data-protection-cases-of-2019-a-selection-suneet-sharma/ accessed on 27th June 2021.

that searches or access by public authorities could only be achieved upon production of search warrants issued by a Judicial officer upon evidence on oath of the inevitability for such warrants.[210]

The foregoing protection of the right to privacy has equally been developed by the Court in various decisions following the enactment of the Constitution of Kenya, 2010. For instance, the Court in *Director of Public Prosecutions v Tom Ojienda t/a Prof Tom Ojienda & Associates Advocates & 3 Others*[211] held that the right to privacy entitles an individual to have control over his personal data and that this right to privacy is to be shielded from unwarranted intrusion. Furthermore, the Court in that matter held that the right to privacy cannot be claimed by third parties on behalf of aggrieved individuals.[212]

The High Court in ***Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others,*** outlined the importance of the right to privacy while outlining how new threats have emerged due to the development of technology and the preparation required to tackle the same. The Court in this decision thus accepted constitutional and common law rights to privacy and moved ahead to interrogate emerging challenges on the basis that the individual's autonomy must be sought after in light of his association with the rest of society.[213] It is therefore considered that the constitutional right to privacy of an individual within a digital cyberspace where finance is involved governs all aspects of life thus there is a need to balance the needs/opportunities with the dangers posed to liberty within that cyberspace.

[210] Vitu Limited vs. The Chief Magistrate Nairobi & Two Others, High Court Misc. Criminal Application No. 475 of 2004
[211] Director of Public Prosecution v Prof. Tom Ojienda & Associates Advocates & 3 Others [2019] eKLR
[212] Director of Public Prosecution v Prof. Tom Ojienda & Associates Advocates & 3 Others [2019] eKLR
[213] Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others Constitutional Petition No. 86 of 2017

The Court in that matter therefore suggested that this balancing act can only be achieved if the aspect of data processing is understood as this aspect of data processing includes the collecting, storage and use of data.[214] Thus, the distribution of person consumer data is a threat to that consumer's privacy while the acquisition and disclosure of false or misleading information may lead to an infringement of the consumer's identity.

The Court therefore has urged for the strict protection of privacy in online data processing in Fintech transactions. In arriving at its decisions, the Court placed heavy reliance on decisions from the United States, Australia, South Africa, European Union, International Convention and Treaties.[215] From that decision, it was evident that at the time of judgment, there was a limited legislation on privacy thus hindering the full realization of the constitutional right to privacy and protection of data in Fintech transactions.

3.7 Conclusion

While it commendable that Kenya now has in place a legal framework, vide the Data Protection Act, to govern various financial transactions that take place over technological platforms, the said Act has been criticized for not being sufficient to regulate research data.[216] Similarly, compliance with the Act will require the use of research practices such as the use of consent and anonymisation in order to safeguard personal data. The Regulations, once the same is enacted, will bring much

[214] Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others Constitutional Petition No. 86 of 2017

[215] Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others [2018] eKLR

[216] https://theconversation.com/how-kenyas-new-personal-data-protection-law-could-affect-researchers-153558#:~:text=Passed%20in%202019%2C%20the%20Kenya,thus%20strengthening%20individuals%20fundamental%20rights. Accessed on 10th May 2021.

clarity to any shortcomings that may have arisen from the Data Protection Act within Fintech transactions.

Thus, while the Data Protection Act has good intentions and states the principles of data protection while balancing the principles of data protection and the rights of consumer vis-à-vis actions of Fintech service providers, the said Act is still insufficient as it still does not have effective mechanisms for the enforcement of those principles of data protection and rights of the consumers in spite of attempting to replicate prevailing international standards.

Chapter Four: Protection of Consumer Data in Fintech Transactions in The United Kingdom

4.1 Introduction

In the United Kingdom, the concept of privacy, particularly in the Fintech arena, is a multi-faceted one. Nonetheless, various scholars have made attempts to confine the concept of privacy within the Fintech arena to one single definition. For instance, Warren and Brandise have stated that the right to privacy is principally based on the "*inviolate personality of a person*" making basis of privacy to be one's control over his/her own information.[217]

However, despite the running argument as has been earlier set out in this thesis that there is a natural link between the right to privacy and the right to data protection, a strong case has been made regarding the disconnect between data protection and privacy on the basis of the contents of Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union to which the United Kingdom is a party to.[218] Article 7 of the Charter sets out the right to respect one's private and family life which includes one's home and communications. Article 8 on the other hand, guarantees the right to the protection of personal data concerning oneself. It is on this basis that the parameters that will be compared between the United Kingdom and Kenya is the regulatory frameworks between the two jurisdictions especially so as to determine the regulatory safeguards put in place within the United Kingdom.

4.2 The Constitutional Framework governing the processing of personal data

The United Kingdom is a Parliamentary Democracy with a constitutional sovereign as Head of State. It equally has a sovereign Parliament which is superior to other government institutions. The

[217] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, as cited in Judith DeCew, 'Privacy', The Stanford Encyclopedia of Philosophy, Spring 2015 <https://plato.stanford.edu/archives/spr2015/entries/privacy/> accessed 5th May 2021.

[218] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Executive of the United Kingdom is equally drawn from and is accountable to this sovereign Parliament as well as an independent judiciary. Additionally, the UK parliament has delegated part of its legislative responsibility to the Scottish Parliament, the Welsh Parliament (*Senedd Cymru)* and the Northern Ireland Assembly for legislating on domestic matters within Scotland, Wales and Northern Ireland. Data Protection is however a matter reserved specifically for the sovereign Parliament.[219]

It must be noted that the United Kingdom does not have a codified constitution in the sense of an entrenched constitutive document. Therefore, within the UK, Constitutional principles have emerged over time, drawn from case law and convention in particular. Equally, the constitutional value of certain statutes have been recognized by the Courts.[220] It is through these statutes, common law and international treaties[221] that fundamental rights and freedoms including those touching on data protection and privacy, have been developed. The United Kingdom has further ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[222]

The Human Rights Act of 1998 domesticates within the UK the rights contained in the European Convention on Human Rights. This Act grants any individual the fundamental rights and freedoms which are provided for from Article 2 through to Article 12 and 14 of the European Convention on Human Rights, Articles 1, 2 and 3 of that Convention's First Protocol as well as Article 1 of

[219] This has the net effect that the same legislation on data protection applies throughout the UK.
[220] These include the Magna Carta, the Bill of Rights 1689 and the Human Rights Act 1998.
[221] In particular the European Convention on Human Rights which the United Kingdom ratified in 1951.
[222] The principles of Convention 108 had been initially enacted into the United Kingdom legal framework vide the Data Protection Act, 1984, which was subsequently repealed and replaced by the Data Protection Act of 1998 and subsequently the Data Protection Act of 2018 (as read with the UK GDPR). The United Kingdom has also signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Known as Convention 108+) in 2018 and is in the process of ratifying the said Convention.

that Convention's Thirteenth Protocol, which provisions are read together with Articles 16, 17 and 18 of the Convention. This includes the right to respect for private and family life, which is a right that is easily infringed in Fintech transactions. In particular, in compliance with Article 8 of that Convention, a public authority may only interfere with the right to privacy conformity with the law, where necessary in a democratic society and in the interests of national security, public safely or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. It must be noted that under the Human Rights Act, 1998, the actions of state agencies are required to be compatible with a Convention Right.[223]

Within the United Kingdom, the General Data Protection Regulation 2016/17 (GDPR)[224] sets out the subjective rights and obligations which are to be protected within the United Kingdom. These include an anticipation that competing interests of consumers, controllers and third parties will be equally and equitably balanced, that standards, which include data minimization and accuracy will be observed, that data use will be transparent and that consumers are able to exercise a certain degree of control over processing especially when the data and/or context is of a sensitive nature.[225] The GDPR builds on the former Data Protection Directive (DPD) 95/46[226] and sets forth a number

[223] Section 6, Human Rights Act, 1998.
[224] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 EC (General Data Protection Regulation) [2016]
[225] Erdos D, 'Ensuring Legal Accountability of the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?' (2020) 6 European Data Law Review, vol. 6, no. 3, 2020, pg. 3
[226] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individual with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

of answers to the question of data protection within Fintech transactions including permitting persons to pursue private actions for injunctive or compensatory relief in the event of breach.[227]

An essential part of the GDPR's framework is that it grants data subjects/consumers the ability to reach out to Statutory Data Protection Authorities (DPAs). The principal aim of data protection provisions within the GDPR

4.3 Principal Changes brought forth by the GDPR

In order to fulfil the aims for which it was granted, which essentially is to create a balance between protection of the fundamental rights of data of consumers and freedom of flow of such personal data throughout the European Union, the GDPR makes provision for numerous innovations in processing personal data, which is as below:

4.3.1 GDPR extends its territorial application

The provisions of the GDPR are applicable to all processing of consumer data "*in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing itself takes place within the Union or not*."[228] This is further expanded by Article 3(2) of the GDPR which refers to all non-EU data controllers and data processors/Fintech service providers but which nonetheless offer goods/services to European data subjects and consumers or which monitor their behavior. This, grants specificity to the GDPR over the DPD which only placed reliance on '*equipment/means'*.

4.3.2 Principles of transparency and accountability

The GDPR requires that collected data ought to be processed "*in a transparent manner*"[229] and further requires that data which is inaccurate must be immediately deleted or rectified.[230]

[227] Article 76, GDPR
[228] Article 3(1) GDPR
[229] Article 5(1)(a) GDPR
[230] Article 5(1)(d) GDPR

Furthermore, the GDPR progresses the accountability principle which requires absolute compliance upon the data controller/Fintech service provider which is expected to also demonstrate that compliance. Thus, Fintech service providers are expected to keep comprehensive records of their data processing activities and to take suitable technical and organizational steps to guarantee data protection by design and by default which can be verified by certification through the means provided for under Article 42 of the GDPR.

4.3.3 Lawfulness of Data Processing

The GDPR places emphasis on the need for legitimacy for processing of personal data as envisaged by statute or with the prior consent of the consumer.[231] The consumer must be able, and without coercion, '*to freely give "specific, informed and unambiguous consent'* for each transaction involving processing of their data. The consumer must also be permitted to withdraw their consent at any stage of the data processing in an easy manner.[232] Thus, a Fintech service provider is expected to demonstrate that the consumer of the Fintech service has givesn his/her prior consent.

In relation to the age of the consumer, the processing of personal data of persons under the age of 16 is only permitted and to the extent that prior consent is issued or permitted by the holder of parents or guardians of the child.[233] The Fintech service provider is thus expected to make reasonable efforts to confirm that the consumer has issued prior consent or authorized consent.[234]

4.3.4 Specific rights that are enjoyed by the Fintech Consumer

Following the coming into force of the GDPR, the Consumer of Fintech services in the UK have exerted more control over the processing of their personal data. The GDPR has also resulted in UK Fintech consumers enjoying certain new rights including the right to restrict the processing of

[231] Article 6(1) GDPR
[232] Article 7 GDPR
[233] Article 8(1) GDPR.
[234] Article 8(2) GDPR

their data, the right to data portability, rights in relation to automated decision making and profiling as the right to have their data erased upon request.[235]

It is thus expected that the Fintech service provider will inform the data subject/consumer of the rights accruing to them and how the consumer will be able to enjoy those rights.[236] Thus, the Fintech service provider is expected to provide any information and communication referred to the data processing "*to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided*." This information ought to be given in writing or by other appropriate means such as electronic means.[237]

Additionally, the Fintech service provider is expected to enable the exercise of consumer rights and thus "*shall not refuse to act on the request of the data subjects for exercising their rights, unless the controller demonstrates that it is not in a position to identify the data subject."*[238] In such a scenario, it is expected that the Fintech service provider will provide information on action taken on a request to the consumer without any unnecessary delay and within one month of receipt of the request.[239] During this entire process, the Fintech service provider is expected to provide a copy of the personal data undergoing processing.[240] The UK may however place restrictions upon certain rights of data subjects so long as the said restrictions are necessary and proportionate as what is required in an open and democratic society to protect national interests.[241]

[235] Motatu A., Miltaru I. Diversity and Interdisciplinarity in Business Law (Adjusris.,2017) 5.
[236] Article 15(1) GDPR
[237] Article 12(1) GDPR
[238] Article 12(2) GDPR
[239] Article 12(3) GDPR
[240] Article 15(3) GDPR
[241] Article 23 GDPR

4.3.5 Notification of Data Breach

The GDPR has introduced a mandatory data breach notification mechanism which places an obligation upon the Fintech service provider to immediately report any personal data breaches to the relevant data protection supervisory authority except in circumstances where the breach will most likely not result in a risk to the rights and fundamental freedoms of the consumers. However, in circumstances where the risk is high, then the Fintech service providers are required to also promptly inform their data subjects of the said breach.[242]

4.4 The Enforcement mechanisms under the GDPR

Article 51 of the GDPR outlines on the enforcement mechanisms which may be exercised by regulators in respect to protection of consumer data in Fintech transactions. At a national level, member states, including the UK were obligated to have at least one independent public body with the specific mandate of monitoring the application of the GDPR within that member state. On a regional level on the other hand, member states are expected to coordinate and cooperate in order to guarantee that there is uniform application of the GDPR as well as formulating a consistency mechanism that would guide those member states domestic enforcement.[243]

In addition to member states being obligated to put in place domestic legislative framework to govern the protection of data of consumers in Fintech transactions as well as the right to privacy, member states are also obligated to notify the Commission with the provisions of its laws adopted pursuant to data protection by the date of the enforcement of the GDPR and any subsequent amendment on the domestic legislation.[244]

[242] Article 34 GDPR.
[243] Article 63, GDPR.
[244] Article 51, GDPR.

The supervisory authorities under members states are expected to have both investigative powers as well as corrective powers. The investigative powers include, but are not limited to:

i. To order the Fintech service provider, its agents, servants and/or representatives to provide any data which will be necessary for the regulatory authority to perform its duties;

ii. To conduct data protection audits of Fintech service providers as a method of investigations.

iii. To conduct a review of certifications issued to Fintech service providers.

iv. To notify the Fintech service providers of an alleged infringement of the GDPR.

v. To gain access to any premises occupied by a Fintech service provider, including data processing equipment as long as that access is in accordance with the member state's domestic legislation on access of premises.

The corrective powers[245] on the other hand include the following:

i. To issue warnings to a Fintech service provider when their intended processing operations are likely to infringe provisions of the Regulation.

ii. To issue reprimands to a Fintech service provider where processing operations have actually infringed provisions of the Regulation.

iii. To order the Fintech service provider to acquiesce with the consumer's requests to exercise the rights provided for within the Regulation.

[245] Article 58 of the GDPR

iv. To order the Fintech service provider to ensure compliance with provisions of the Regulation where necessary in its operation, within a specified period and in a specified manner.

v. To order the Fintech service provider to communicate a personal data breach to the consumer.

vi. To order the rectification or deletion of personal data or restriction of processing and the notification of such other actions to the consumers who have had their personal data breached.[246]

vii. To withdraw the certification of a Fintech service provider or to order a certification body not to issue certification where the requirements have not been met or are no longer met.[247]

viii. To impose an administrative fine among other measures based on the circumstances of each individual case.[248]

ix. To order the suspension of data flows to a recipient in a third country or to an international organization.

4.5 Applicability of the GDPR Post-Brexit

It must be noted that the EU GDPR does not apply in the United Kingdom after the end of the Brexit Transition period which had been slated for 31st December 2020.[249] It must however be noted that the United Kingdom's Data Protection Act has already enacted the EU GDPR provisions

[246] This is provided for under Articles 16,17, 18 and 19 of the GDPR.
[247] This power to withdraw certification or to have a certification body withdraw certification is provided for under Articles 42 and 43 of the Regulation.
[248] Article 83, GDPR.
[249] https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr accessed on 1st May 2021

into United Kingdom law. Furthermore, from 1st January 20202, the **DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU) Exit)) Regulations** amended the Data Protection Act of 2018 and combined it with the provisions of the EU GDPR to form a new, UK Specific Data Protection regime known as the UK GPDR.[250] This UK-GDPR is essentially the same as the European GDPR.

Brexit will without a doubt have serious implications for data protection within the UK and specifically the continuous flow of data from the EU to the UK.[251] As has been indicated above, data protection, in the Fintech arena in the UK was governed by the EU General Data Protection Regulations 2016/679 (GDPR) which had been domesticated in the UK through the UK Data Protection Act. Once the UK withdrew from the UK using the deadline set, the Data Protection Act as read together with the **European Union (Withdrawal) Act, 2018**,[252] became the legal framework which incorporated the GDPR into UK Law.

As of March 2018, the UK and the EU had reached political consensus on the stipulations and requirements of a transitional period that commenced on March 29, 2019 and ended on 31st December 2020.[253] Apart from the fact that the UK Data Protection Act would incorporate the provisions of the GDPR into UK law, it was agreed that during that intervening transitional period of March 29, 2019 and December 31, 2020, that the common EU Rules, which also include the GDPR, would still be applicable within the UK during that period.

[250] https://www.legislation.gov.uk/uksi/2019/419/introduction/made accessed on 1st May 2021
[251] Long, W. and Bluthe F. Data Protection and Post-Brexit Issues 2 International Data Protection Officer, Privacy Officer and Privacy Counsel, 8 (2018).
[252] This is the principal legislative framework governing the UK's withdrawal (Brexit) from the EU.
[253] Long, W. and Bluthe F. Data Protection and Post-Brexit Issues 2 International Data Protection Officer, Privacy Officer and Privacy Counsel, 8 (2018).

4.5.1 International Transfers Post-Brexit

As had already been delineated within this Chapter, the GDRP prohibits the transfer of personal data of consumers to third parties. The only exception to this general rule is where the transfer of the personal data to third countries is made to an "*adequate jurisdiction*"; or where the Fintech service provider, who is exporting the said data has put in place a lawful and valid data transfer mechanism which can, for instance, be the EU Standard Contractual Clauses, Binding Corporate Rules or the EU/Swiss-Privacy Shield; or in circumstances where exemption or derogation under the GDPR is expressly provided for. The effect of the exit from the EU on 29th March 2019, the United Kingdom was considered to be a third country and the consequence of such consideration is that the transfer of personal data by Fintech service providers in the EU to the UK were required to either satisfy that the transfer was made to an "adequate jurisdiction" or an exemption or derogation under the GDPR was applicable.[254] It is the above exceptions that will be discussed hereinafter:

4.5.2 Adequacy Decision

Sometime in May 2018, the UK Government issued a position paper containing what it proposed as a way forward for a post-Brexit data agreement. Within that position paper, the UK sought a legally binding agreement that would permit EU-UK data flows after Brexit had been done and dusted. It was envisaged that this legally binding agreement could not be unilaterally changed by the EU.[255] This proposal was however rejected by Michael Barnier, who served in the capacity as Chief Brexit Negotiator, on the grounds that the proposed framework went beyond the standard adequacy approach that the EU had given other countries.

[254] Long, W. and Bluthe F. Data Protection and Post-Brexit Issues 2 International Data Protection Officer, *Privacy Officer and Privacy Counsel,* (2018), 8.

[255] Long, W. and Bluthe F. Data Protection and Post-Brexit Issues 2 International Data Protection Officer, Privacy Officer and Privacy Counsel, 8.

It must be noted that despite in theory, an adequacy decision being attainable given the fact that the UK recently domesticated the GDPR through the UK Data Protection Act which ideally ought to be considered as an "*essential equivalent*" to the EU, whether or not the same is adequate seems to be a much broader question than whether there is a data protection legislation. Specifically, where the UK is required to seek a post-Brexit adequacy decision from the European Commission, there is an expected that its present surveillance regime, which also includes the UK Investigatory Powers Act 2016, would come under close scrutiny. Indeed, the European Court of Human Rights recently rendered its decision in ***Big Brother Watch and Others v. The United Kingdom***.[256] In that decision, the European Court of Human Rights arrived at a finding that UK law enforcement authorities had participated in bulk interception of private electronic communications without having put in place sufficient safeguards against the violation of fundamental rights. This, in the view of the European Court of Human Rights, was likely to complicate matters further.

4.5.3 Standard Contractual Clauses.

On or about September 2018, the UK Government issued a technical notice dubbed 'Data Protection if there is not Brexit deal'. This technical notice designs various actions that UK based entities are expected to take in order to guarantee the continued flow of consumer data in Fintech transactions between the UK and the EU especially in the circumstance where the UK would leave the EU with no exit agreement in place. Specifically, the UK Government proposed that entities ought to use standard contractual clauses (SCCs) as the primary mode of legitimizing transfer of personal consumer data from the EU to the UK especially where the UK is the data importer. This technical notice however failed to address both the transfer of personal data from the UK to the US which was to be done in relation to the EU-US Privacy Shield. The technical notice further

[256] [2018] ECHR

failed to address the onward transfer from the UK of personal data which has been received from the EU to a third country such as Kenya.

4.6 Conclusion:

Despite the UK Data Protection Act 2018 majorly adopting and domesticating the GDPR, there is still much uncertainty regarding post-Brexit international transfer of data collected in Fintech transactions. What has actually been recommended is that organizations do review their current data transfer programmes and independently and widely consult on what steps ought to be taken to minimize any post-Brexit disruption of data flows.

From the moment the GDPR came into force, all actors, including those in the Fintech arena within the UK have been forced to comply with it. In this regard, the GDPR has made Fintech service providers within the United Kingdom to comply with all internal procedure for handling personal data in order to cover all requests placed by Fintech consumers, to implement procedures regarding data breaches, and, generally, to protect natural persons with regard to the processing of their personal data.

Chapter Five: Conclusion and Recommendations

5.1 Conclusions

Chapter two of this thesis established that it is evident that Fintech service providers are to be held to an information fiduciary standard as one of the means which will guarantee data-focused business models can continue to operate while the consumers remain to be adequately protected. This would be achieved through four principles being anti-manipulation, antidiscrimination, limited third party sharing and holding companies to their own privacy policies. With the constant evolution of technology which is used in finance, there is a need to safeguard privacy standards of Fintech entities towards their consumers who may have varying expectations in terms of protection of their data.

Chapter Three has established that Kenya now has in place a legal framework to govern the protection of data over various financial transactions that take place over technological platforms. There is however need to ensure compliance with the said Act through the enactment of the Regulations to bring clarity to shortcomings that may have risen from the Data Protection Act within Fintech transactions.

Chapter four of this thesis has established that despite the UK Data Protection Act 2018 majorly adopting and domesticating the GDPR, there is still much uncertainty regarding post-Brexit international transfer of data collected in Fintech transactions. This Chapter has demonstrated however that the GDPR has made Fintech service providers within the United Kingdom to comply with internal procedures for handling of personal data in order to cover all requests placed by Fintech consumers and to further put in place procedures that would govern data breaches and serve to protect natural persons with regard to the processing of their personal data.

5.2 Recommendations

To this end, the following recommendations would suffice to ensure that consumer data in Fintech transactions in Kenya is adequately protected. First among these recommendations is the need to have supervisory authorities in Kenya to have both investigative and corrective powers as has been demonstrated to exist in the United Kingdom. These investigative powers can be incorporated within the Regulations which will give effect to the Data Protection Act. The investigative powers would include, but would not be limited to: ordering the Fintech service provider, its agents, servants and/or representatives to provide any data which will be necessary for the regulatory authority to perform its duties; conducting data protection audits of Fintech service providers as a method of investigations; conducting a review of certifications issued to Fintech service providers; notifying the Fintech service providers of an alleged infringement of the GDPR; and gaining access to any premises occupied by a Fintech service provider, including data processing equipment as long as that access is in accordance with the member state's domestic legislation on access of premises.

The corrective powers which may be included within the Regulations will include: issuing warnings to a Fintech service provider when their intended processing operations are likely to infringe provisions of the Regulation; issuing reprimands to a Fintech service provider where processing operations have actually infringed provisions of the Regulation; ordering the Fintech service provider to acquiesce with the consumer's requests to exercise the rights provided for within the Regulation; ordering the Fintech service provider to ensure compliance with provisions of the Regulation where necessary in its operation, within a specified period and in a specified manner; ordering the Fintech service provider to communicate a personal data breach to the consumer; ordering the rectification or deletion of personal data or restriction of processing and

the notification of such other actions to the consumers who have had their personal data breached;[257] and ordering the suspension of data flows to a recipient in a third country or to an international organization.

A second recommendation which ought to put into consideration is the enactment of proposed Regulations which are already in the pipeline. Even though these Regulations are a form of delegated legislation, they still provide administrative and technical detail to carry out the intended purpose and principles of the Data Protection Act.[258]

[257] This is provided for under Articles 16,17, 18 and 19 of the GDPR which may be incorporated into the Kenyan Context in the Data Protection Regulations

[258] The Data Protection Act is an Act of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes.

References

Aloo L.O. 'Mobile Banking in Kenya, Recent Developments – A legal practitioner's perspective' paper presented at UNICITRAL International Colloquium on Microfinance, Vienna, (2011).

Anne Mathew, 'Crowd-Sourced equity funding: The regulatory challenges of innovative Fintech and fundraising special colloquium section' 36 *University of Queensland Law Journal*, 2017, 41.

Anton Didenko 'Regulating FinTech: Lessons from Africa' 19 *San Diego International Law Journal*, 2017, 311.

Anton Didenko, 'Regulatory challenges underlying FinTech in Kenya and South Africa' , Bingham Centre for the Rule of Law, December 2017 available on https://www.biicl.org/documents/1814_regulation_of_fintech_in_kenya_and_south_africa_v_1.pdf accessed on 27 January 2020.

Barnabas Andiva, 'Mobile Financial Services and Regulation in Kenya' *Competition Authority of Kenya* (2014).

Bennett Regulating Privacy: data protection and public policy in Europe and the United States (1992).

Bourdon C, 'Analysis of the FinTech ecosystem: What regulatory and corporate responses could foster the innovation whilst not threatening the financial stability and the consumers' interests ?' *Unpublished LLM Thesis, Tilbury University*, 2017, 53.

Capgemini, *World FinTech Report* 2017 (2017) 12.

Cass R. Sunstein, Fifty Shades of Manipulation 1 Journal of Behaviour (2015).

Charles Wjr Mooney, 'Fintech and secured transactions systems of the future secured transactions law in the Twenty-First century' 81 *Law and Contemporary Problems,* 2018, 1.

Clément Bourdon, 'Analysis of the FinTech ecosystem: What regulatory and corporate responses could foster the innovation whilst not threatening the financial stability and the consumers' interests ?'

Claudia NG, Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy, available on https://www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy accessed on 13th December 2020.

Chris Brummer and Yesha Yadav, 'Fintech and the innovation trilemma' 107 *Georgetown Law Journal*, 2018.

Christopher K Odinet, 'Consumer Bitcredit and Fintech lending' 69 *Alabama Law Review*, 2017.

Christopher G. Bradley, 'Fintech's double edges FinTech's promises and perils' 90 *Chicago-Kenya Law Review,* 2018.

Daniel Heller and Edwin Truman, ‘International financial regulatory cooperation and digital currencies’ 18 *Georgetown Journal of International Affairs*, 2017.

‘Digital Trade: Developing a framework for analysis’ (2017) OECD Trade policy papers 205 <https:www.oecd.ilibrary.org/trade/digital-trade_524c8c83-en> accessed on 22 January 2020.

Dirk A Zetsche and others, ‘From Fintech to Techfin: The regulatory challenges of data-driven finance’ 14 *New York University Journal of Law and Business*, 2017.

Dirk A Zetzsche and others ‘Regulating a revolution: From regulatory sandboxes to smart regulation’ 23 *Fordham Journal of Corporate and Financial Law*, 2017.

Dobkin A. ‘Information Fiduciaries in Practice: Data Privacy and User Expectations. Berkeley Technology Journal 2018.

Douglas W Arner and others, ‘FinTech and RegTech: Enabling innovation while preserving financial stability’ 18 *Georgetown Journal of International Affairs*, 2017.

Douglas W Arner, Janos Barberis and Ross P Buckey, ‘FinTech, RegTech and the reconceptualization of financial regulation’ 37 *Northwestern Journal of International Law & Business, 2016*.

Douglas W Arner, Janos Barberis and Ross P Buckley, ‘The evolution of FinTech: A new post-crisis paradigm’ 47 *Georgetown Journal of International Law*, 2015.

Emberland M. Protection against unwarranted searches and seizures of corporate premises under Article 8 of the European Convention on Human Rights; the Colas Est SA vs. France Approach.

Erdos D, ‘Ensuring Legal Accountability of the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?’ (2020) 6 European Data Law Review, vol. 6, no. 3, 2020,

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Fintech Regulation in Kenya, available on https://www.lexology.com/library/detail.aspx?g=10821111-abdf-4214-a97e-9708fdc36e60 accessed on 13th December 2020.

Florida L. On Human Dignity as a Foundation for the Right to Privacy, Philosophy & Technology Journal, 2016.

Frankenberg G. Human Rights and the Belief in a Just World, 12 Oxford University Journal 2014.

Freund P, Privacy: One Concept or Many, Atherton Press, New York, 1971.

Gordana Golubic ‘Do digital technologies have the power to disrupt commercial banking’ 6 *InterEULawEast: Journal for International and European Law, Economics and Market Integrations*, 2019.

Gkoustzinis A, ‘Internet banking and the law in Europe: Regulation, Financial integration and Electronic Commerce’, *Cambridge University Press*, 2010.

Jack M. Balkin ‘Information Fiduciaries and the First Amendment, 29 University of California at Davis Law Review, 2016.

Jeremy Kidd, ‘Fintech: antidote to rent-seeking FinTech’s promises and perils 93 *Chicago-Kent Law Review*, 2018.

John L Douglas, ‘New wine into old bottles: Fintech meets the bank regulatory world’ 20 *North Carolina Banking Institute*, 2016.

John Pfiffner and R. Vance Prethus, “Public Administration”, *3rd Ed. New York Publishers*, 1953.

Johan den Hertog, ‘General theories of Regulation, Economic Institute.CLAV’, Utrecht University, 1999.

Kariuki J, ‘Mobile banking Services in the East African Community (EAC):Challenges to the existing legislative and regulatory framework’, *4 Journal of Information Policy*, 2014.

Kinuthia and Akinnusi, ‘The Magnitude of Barriers facing eCommerce Businesses in Kenya 2009.

Knight Brian, ‘FinTech: Who regulates it and why it matters’ April 2016 available on https://milkeninstitute.org/sites/default/files/reports-pdf/FinTech-Who-Regulates-It-and-Why-It-Matters2.pdf accessed on 31 January 2020.

Kristina Petljak, ‘Green supply chain management practices in food retailing’ 6 *InterEULawEast: Journal for International and European Law, Economics and Market Integrations*, 2019.

Kutcher R. Breach of Fiduciary Duties, in Business Torts Litigation.

Lenore Palladino, ‘Small business Fintech lending: The need for comprehensive regulation’ 24 *Fordham Journal of Corporate and Financial Law*, 2018.

‘Lexis Library: Document https://www-lexisnexis-com.ezproxy.library.strathmore.edu/uk/legal/results/enhdocview.do?docLinkInd=true&ersKey-23_T29144755310&format=GNBFULL&startDocNo=0&resutsUrlKey=0_T29144755312&backKey=20_T29144755313&csi=385434&docNo=3&scrollToPosition=324 accessed 28 January 2020.

Long, W. and Bluthe F. Data Protection and Post-Brexit Issues 2 International Data Protection Officer, Privacy Officer and Privacy Counsel, 8, 2018.

Magnuson William, ‘Regulating Fintech’ 4 *Vanderbilt Law Review*, 2018.

Malala J, ‘Consumer Law and Policy in Kenya’ 41 *Journal of Consumer Policy*, 2018.

Malala J, Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it presents for mobile payments, WPS/02/14 KBA Centre for research on financial markets and policy working paper series.

Makin P, ‘Regulating Issues Around Mobile Banking: New Initiatives to bank the poor are straining the world’s financial regulatory systems,’ OECD, 2009.

Makulilo A. Privacy and Data Protection in Africa: A state of the Art,’ 2 International Data Privacy Law 2012.

Manuela Geranio, ‘Fintech in the exchange industry: Potential for disruption symposium issue: The British academy and the Ministry of Science and Technology of Taiwan project Titled creating a legal and regulatory framework for interconnections between stock

exchanges: A comparative study of the UK and Taiwan' 11 *Masaryk University Journal of Law and Technology*, 2017.

Martin Meyerson and Edward C. Banfield, "Politics, Planning and the Public Interest" Glencoe, 1955.

Mburu G, 'Case Study Kenya: A regulatory sandbox for the financial sector", published on https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-11/Kenya%20-%20regulatory%20sandbox%20for%20financial%20sector.pdf accessed on 17 August 2020.

Motatu A., Miltaru I. Diversity and Interdisciplinarity in Business Law (Adjusris.,2017)

Mugo M and Kilonzo E, Community-level impact of financial inclusion in Kenya with particular focus on poverty, eradication and employment creation.

Muthiora B, Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Money for the Unbanked.

Nizan Geslevich Packin, 'RegTech, compliance and technology judgement rule FinTech's promises and perils' 93 *Chicago-Kent Law Review*, 2018.

Privacy and Data Protection Practices of Digital Lending Apps in Kenya, 2020, Strathmore University, Center for Intellectual Property and Information Technology Law.

Robert C. Solomon & Fernando Flores, Building Trust: In Business, Politics, Relations and Life, 2001.

Roger Brownsword, 'Regulating Fitness: Fintech, funny money, and smart contracts' 20 *European Business Organization Law Review*, 2019.

Rory Van Loo, ‘Making innovation more competitive: The case of Fintech’ 95 *UCLA Law Review*, 2018.

Roos A. Core Principles of data protection law contained in 39 1The Comparative and International Law Journal of Southern Africa, 2006.

Samuel Warren and Louis Brandeis, ‘The Right to Privacy’ (1890) 4 Harvard Law Review 193, as cited in Judith DeCew, ‘Privacy’, *The Stanford Encyclopedia of Philosophy, Spring* 2015.

Sarah Nyakio “Digital rights; the Present and the Future”, ICJ-Kenya, https://www.icj-kenya.org, Accessed 24 April 2020.

Saule T Omarova, ‘New tech v new deal: Fintech as a systematic phenomenon’ 36 *Yale Journal on Regulation*, 2019.

Serban Andrea, ‘ the Value of privacy: what does the Personal Data Mean to the Data Subject and Businesses? *Current Issues in Business Law Journal* 2018.

Shleifer A, ‘Understanding Regulation’ 11 *European Financial Management*, 2005.

Shulist J, What is the role of regulation in digital finance, 7 August 2018 available on https://www.financedigitalafrica.org/snapshot/what-is-the-role-of-regulation-in-digital-finance/ accessed on 16 August 2020.

Sorauf F, ‘The Public Interest Reconsidered’, 19 *The Journal of Politics*, 1957.

Viktoria Chatzara, ‘FinTech, InsurTech, and the regulators’ available on link.springer.com.ezproxy.library.strathmore.edu accessed on 27 January 2020.

Victoria Smith Ekstrand and Christopher Roush, ‘From hot news to hot data: The rise of Fintech, the ownership of big data, and the future of the hot news doctrine’ 35 *Cardozo Arts & Entertainment Law Journal*, 2016.

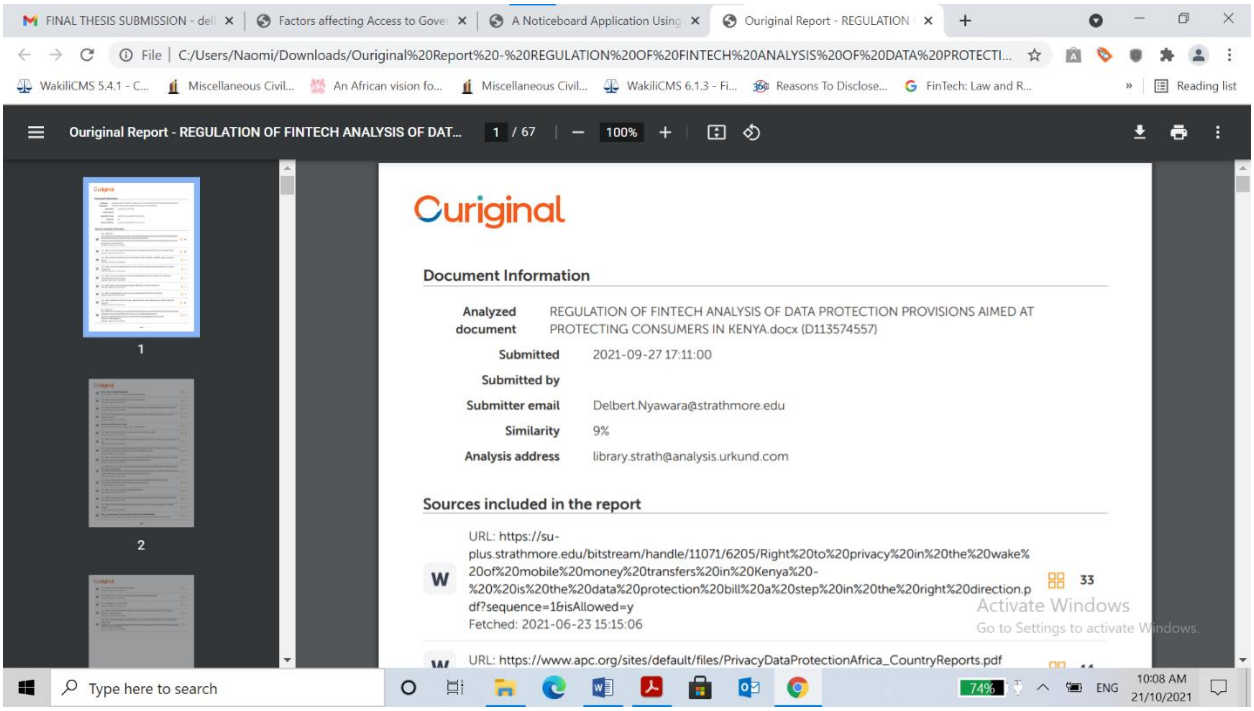
Vicki Waye, ‘Regtech: A new frontier in legal scholarship’ 40 *Adelaide Law Review, 2019*.

V Gerard Comizio, ‘Virtual currencies: Growing regulatory framework and challenges in the emerging Fintech ecosystem’ 21 *North Carolina Banking Institute,* 2017.

Warren S and Brandeis L, “the Right to Privacy” Harvard Law Review, 1980.

6. Appendices

6.1 Appendix A: Similarity Report



6.2 Appendix B: Ethical Clearance Confirmation

Strathmore UNIVERSITY

18th October 2021

Mr Nyawara Delbert,
delbert.nyawara@strathmore.edu

Dear Mr Nyawara,

RE: Regulation of Fintech Analysis of Data Protection Provisions Aimed at Protecting Consumers in Kenya

This is to inform you that SU-IERC has reviewed and **approved** your above SU- **master's** research proposal. Your application reference number is **SU-IERC1170/21**. The approval period is **18th October 2021 to 17th October 2022.**

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-IERC.
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-IERC within 48 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-IERC within 48 hours
v. Clearance for 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 expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to SU-IERC.

Prior to 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 also obtain other clearances needed

Yours sincerely,

for: Prof Fred Were,
Chairperson; SU-IERC

STRATHMORE UNIVERSITY INSTITUTIONAL ETHICS REVIEW COMMITTEE (SU-IERC)
18 Oct 2021
TEL: +254 (0)70303400
P.O BOX 59857-00200
NAIROBI-KENYA

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