Critical Perspectives on Cybersecurity: A Case Study of Legal and Regulatory Responses to Identity-related Cybercrimes in Electronic Payment Systems in Nigeria

Adekemi Olufunmilola Omotubora

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy (PhD)

The University of Leeds
School of Law

July 2015

The candidate confirms that the work submitted is her own and that appropriate credit has been given where reference has been made to the work of others.

This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

Acknowledgements

I am indebted to my supervisors Dr Subhajit Basu and Dr Stefan Fafinski for their critical comments which contributed immensely to my thinking on this project.

I am particularly indebted to my husband, Abayomi Omotubora without whose encouragement and moral and financial support, I would not have started this programme at all. I also acknowledge especially the contributions of my parents Reverend Olalekan Ayangunna and Pastor Abimbola Ayangunna during the course of my PhD programme and indeed throughout my long academic life. I appreciate the support of Mrs Bosede Ikwenobe, a true friend indeed, and my dear bother Adedeji, who always urged me on. I am grateful for the contributions of Senator Solomon Ita-Enang and Dr Rosemary Ita-Enang. I remain grateful to all my friends and family too numerous to mention here, thank you for all your comments, contributions and support.

This thesis is for my dear children Adenile Omotubora and Oluwafikayomi Omotubora.

Abstract

The thesis critically examines the challenges of implementing cybersecurity in Nigeria. It focuses in particular on identity-related cybercrimes in e-payment systems. The thesis follows two broad lines of investigation. First, it examines how the convergence of telecommunications and banking services create a multi-stakeholders' e-payment service provider system and the implications of this convergence for security and regulation of e-payment systems. Second, the thesis examines the societal, institutional and political considerations that affect the legal and regulatory responses to identity-related cybercrimes or that explain the lack of such responses.

The research reveals that social perceptions of cybercrimes and political interference in law making process, as well as lack of proper identity management systems are crucial factors which affect the development and effectiveness of cybersecurity laws in Nigeria. The research also reveals that policy proposals for cybersecurity have focused extensively on criminal legislation and that this approach has marginalised the roles of data protection and identity management laws in preventing identity-related cybercrimes.

The thesis argues that current self-regulatory initiatives in the Nigerian e-payment industry are inadequate due to the multi-stakeholders' nature of electronic transactions. Using Lessig's theory of modalities of regulation as a theoretical framework, the thesis highlights the primacy of laws in defining privacy and security standards as well as technical standards for the protection of users of e-payment services. The thesis however concludes that although laws are crucial, and cybercrimes are global, the development of cybersecurity laws must be moderated by an understanding of the legal and regulatory challenges as well as the socio-cultural and political factors in Nigeria. The thesis makes specific recommendations for developing laws and policies on cybersecurity in Nigeria.

Table of Contents

Acknowledgements ..... **iii**
Abstract ..... **iv**
Table of Contents ..... **v**
Table of statutes ..... **xi**
List of Tables and Figures ..... **xiv**
List of Abbreviations ..... **xv**
1 Introduction **1**
1.1 Central Thesis and Contribution to Knowledge 2
1.2 Principal Research Questions 3
1.3 Chapter Structure and Synopsis 3
1.4 Research Methodology 6
1.4.1 Documentary Research 6
1.4.2 Empirical Study 7
1.5 Research Ethics- Informed Consent and Data Protection 11
1.6 Data Analysis 12
1.7 Generalisability of Findings 14
1.8 Limitations of the Research 16
2 Legal and Institutional Frameworks for E-payment Systems in Nigeria **17**
2.1 PART I - An Introduction to the Nigerian Legal System 17
2.1.1 Sources of Law 17
2.1.2 Constitutional Framework 18
2.1.3 The Legislative Process 19
2.1.4 The Judicial System 20
2.2 Part II- Overview of E-Payment Systems in Nigeria 21
2.2.1 Development of Banking and Payment Systems in Nigeria 21
2.3 Legal Aspects of E-Payments 23
2.3.1. What is E-Payment (Systems)? 23
2.3.2 Legal Status of E-payments 25
2.3.3 Money as a Social Construct 28
2.3.4 Classifications of E-payment Systems 31
2.4 E-payment Systems and Development in Nigeria 41
2.4.1 Consumer Convenience 41
2.4.2 Reduction in the Cost of Cash 42
2.4.3 Promoting Financial Inclusion 42
2.4.4 Developing E-commerce 43
2.4.5 Controlling Crime 46
Conclusion 46
3 Cybercrime Threats to E-payment systems **48**
3.1 Internet Fraud in Nigeria 48

3.2 The Challenges of Fraud Reporting 50
3.3 Identity Related Cybercrimes 51
3.3.1 What is (Digital) Identity? 52
3.3.2 Threat Vectors and Activities 56
3.4 Criminal Misuse of Identity Information 70
3.4.1 Account Takeover Fraud 70
3.4.2 Internet Banking Fraud 71
3.4.3 Card Not Present Transaction Fraud 72
3.4.4 SIM Swap Fraud 72
3.5 Industry Responses to cybercrime Threats –Private Ordering and Technical Security Standards 73
3.5.1 Central Bank of Nigeria (CBN) Regulations on Privacy and Security 73
4 Criminal Law Responses to Identity-related Cybercrimes 87
4.1.1 (Not) Defining Cybercrime 88
4.2 Hacking under the Criminal Laws 92
4.2.1 Hacking as Trespass 92
4.2.2 Hacking as Damage to Property 93
4.2.3 Hacking Offences under the Cybercrime Bill 2014 96
4.3 Phishing- Fraudulent Representation and Computer-related Fraud 112
4.3.1 The Nigerian Criminal Law on Phishing, False Pretence and Electronic Payment Fraud 112
4.3.2 Computer Fraud under the Cybercrime Bill 119
4.4 Spamming, Malware Distribution and Modification and Damage of Computer Programs 121
4.5 Identity Theft and Identity Fraud under the Criminal Code Act and the Cybercrime Bill 123
4.6 Administration and Enforcement under the Cybercrime Bill 129
4.6.1 Lack of Computer Forensics Capacity in Law Enforcement 130
4.6.2 The Politics of the “Fight for Turf” 132
Conclusion 133
5 Data Protection in Nigeria 135
5.1 Challenges of Data Protection in E-payment Systems in Nigeria 135
5.1.1 NIMC’s Electronic National Identity Card 137
5.1.2 NCC SIM Registration 138
5.1.3 CBN Bank Verification Number (BVN) 139
5.2 Regulation of Data Processing in Nigeria – Laws, Regulations and Guidelines 140
5.2.1 Constitutional Provisions on Privacy Protection 141
5.2.2 Freedom of Information Act 2011 145
5.2.3 Guidelines on Data Processing in Telecom and Banking Sectors 145
5.2.4 Draft Law on Data Protection- Information Privacy and Data Protection Bill 2013 148
5.3 Meaning and Scope of Personal Information in Nigeria 149

5.3.1. Definitions of Personal Information under Laws and Regulations in Nigeria....149
5.4 Challenges of Enactment, Administration and Enforcement of Data Protection Law 164
5.4.1 Institutional lobby against legislating on data protection 165
5.4.2 Non-compliance with Regulation- 'The Culture of Impunity' 167
5.4.3 Challenges of Identity Management 169
6 Theories of Regulation in Cyberspace 174
6.1 Regulation Generally 174
6.2 The Cyberlibertarian and Cyberpaternalist Theories of Regulation in Cyberspace 177
6.3 Lessig's Theory of Modalities of Regulation 182
6.4 The Limits of Technology, Industry and Users in Controlling Identity-related cybercrimes in e-payment systems in Nigeria 188
6.4.1 The Limits of Technology (Code) Regulation....188
6.4.2 Market Regulation and Constraints of the Payment Industry 195
6.4.3 The Law and Regulation of Users 205
Conclusion 214
7 A Proposal for Cybersecurity for E- payment Systems in Nigeria 215
7.1 Statement of the Proposal 215
7.2 The Scale of the Problem - Identity-related Cybercrimes are Pervasive . 216
7.3 The Challenges of Criminal Legislation 217
7.3.1 Social Perceptions of Cybercrime....218
7.3.2 Legislative Delays....219
7.3.3 The "Fight for Turf" Among Law Enforcement Agencies in Nigeria 220
7.4 Understanding the Limits of Legal and Regulatory Frameworks.... 221
7.4.1 Cybercrime Bill 2014- Intractable Challenges of Enforcement and Effectiveness 222
7.4.2 Regulation of Data Processing- The Privacy and Data Protection Bill 2013....223
7.4.3 Laws that Regulate (effectively) Criminal (Reactive) Law vs Non-Criminal Legislation 225
7.5 Recommendations for Achieving Cybersecurity in E-payment Systems in Nigeria.... 228
7.5.1 Enactment of Cybersecurity Laws for Electronic Transactions....229
7.5.2 Creation of Specialised Agency for Cybersecurity....233
7.5.3 Capacity Development in Computer Forensics 235
7.5.4 Centralising Identity Management Program....236
7.5.5 Integration of Regulatory Impact Assessment into Decision Making Process of Government 238
7.5.6 Effective Implementation of National Cybersecurity Strategy- Understanding Private/ Public Partnership as an advantage with a Caveat239
7.5.7 Public Awareness and Education....244
Conclusion 244

8 Conclusion of Central Thesis 246
8.1 Revisiting the Research Question 246
8.2 Broader Application of Research 251
Bibliography 252
Appendix 261

Table of cases

Canada (Information Commissioner) v Canada (Transportation Accident Investigation & Safety Board) 2006 FCA 157

Cox v Riley (1986) 83 Cr App R 54

Dagg v Canada (Minister of Finance) [1997] 2 S.C.R 403

Digital Rights Ireland Ltd v Minister for Communications Marine and Natural Resources [2014] All ER (D) 66 (Apr)

DPP v Bignell [1998] 1 Cr App R 1

Durant v Financial Services Authority [2003] EWCA Civ 1746

Eastmond v Canadian Pacific Railway (2004) 33 CPR (4^{th}) 1

Englander v Telus (2004) 247 D.L.R (4th) 275

Federal Republic of Nigeria v Amadi (2006) 1 EECLR 15

Federal Republic of Nigeria v Fani-Kayode (2010) 14 NWLR 481

Federal Republic of Nigeria v Yaro (2012) 3 SCNJ 236

Foskett v Mckeown (2001) 1 AC 102

Gordon v Canada (Minister of Health) [2008] FC 258

Holmes v Governor of Brixton Prison (2004) EWCH 2020 (Admin)

Job v Halifax PLC (unreported)

Kingsley v Sterling Industrial Securities Ltd (1966) 2 All ER 414

Leon's Furniture Limited v Alberta (Information and Privacy Commissioner [2011] ABCA 94

Medical and Dental Practitioners Disciplinary Tribunal v Dr John Emewulu Nicholas Okonkwo (2001) 7 NWLR Pt 711

Mike Amadi v Federal Republic of Nigeria (2008) 12 SC (pt III) 55

Morphitis v Salmon (1990) Crim. LR 48

Onagoruwa v The State (1993) 7 NWLR (Pt 303)

Oxford v Moss (1979) 68 Cr App R 183

Alberta Statutes (Re) [1938] SCR 100

R v Charles (1977) AC 177

R v Bedworth (unreported) 1991

R v Cuthbert (unreported)

R v Delaware (Ian) [2003] EWCA Crim 424

R v Gold & Schifreen (1988) 1AC 1063

R v Gold (1987) 3 All ER 618

R v Hardy Attorney General's Reference (No 1 of 2007) 2007 All ER (D) 102 (Mar)

R v Lambie [1981] 1 All ER 332

R v Preddy (1996) 3 All ER 481

R v Whiteley (1991) 93 Cr App R 25

Sinclair v Brougham (1914) AC 398

State v Allen 917 P 2d 848 (Kan 1996)

State v Riley 846 P 2d 1365 (Wash 1993)

Suffel v Bank of England (1882) 9 QBD

Tournier v National Provincial and Union Bank of England [1924] 1 KB 461

Uzoka v Federal Republic of Nigeria (2009) LPELR -4950 (CA)

Wales Shojibur Rahman v Barclays Bank PLC (unreported)

Welham v DPP (1961) AC 103

White v Elmdene Estates Limited (1960) QB 1

Yesufu v ACB 1 All NLR (Pt 1) 264

Table of statutes

Nigeria

Advance Fee Fraud and Other Related Offences Act 2006

Banks and Other Financial Institutions Act 1991

Central Bank of Nigeria Act 2007

Constitution of the Federal Republic of Nigeria 1999

Criminal Code Act 1916

Cybercrime Act 2015

Economic and Financial Crimes Commission (EFCC) Establishment Act 2004

Evidence Act 2011

Freedom of Information Act 2011

Nigeria Identity Management Commission (NIMC) Act 2007

Nigerian Deposit Insurance Commission Act 2006

Penal Code Act 1959

United Kingdom Legislation

Computer Misuse Act 1990

Consumer Credit Act 1974

Criminal Damage Act 1971

Data protection Act 1998

Forgery and Counterfeiting Act 1981

Fraud Act 2006

Identity Cards Act 2006

Identity Documents Act 2010

Theft (Amendment Act) 1996

Statutory Instruments

Electronic Money Regulation 2011 SI 2011/99

Payment Services Regulations 2009 SI 2009/209

EU Regulations and Directives

Council Directive (EC) 95/46 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data [1995] OJ L281

Council Regulation (EU) No 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market [2014]

Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such data (General Data Protection Regulation) (COM(2012) 11 final

Canadian Legislation

Personal Information Protection and Electronic Documents Act 2000

United States

Electronic Fund Transfer Act 15 USC 1601

Gramm-Leach Bliley Act 12 USC 1811

Health Information Portability and Accountability Act 42 USC 201

Identity Theft and Assumption Deterrence Act 18 USC 1028

Council of Europe

Council of Europe ETS No 185 Convention on Cybercrime 2001

Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of acts of a Racist and Xenophobic Nature Committed through Computer Systems 2003

Council of Europe Convention for the Protection of the Individual with regard to Automatic Processing of Personal Data (ETS no 108) 1981

African Union

African Union Convention on Cybersecurity and Personal Data Protection African Union Legal Instrument LC12490 [2014]

United Nations

Universal Declaration of Human Rights 1948

Bills

Computer Security and Protection Bill 2009 (HB 321) C 3681

Cybercrime Bill 2014 [SB 669]

Cybersecurity Bill 2011 (HB 154) C4443

Economic and Financial Crimes Commission (Establishment) (Amendment) Bill 2010 (HB 351) C 349

Payment Systems Management Bill 2009

Personal Information and Data Protection Bill 2013

List of Tables and Figures

Table 3.1 sample spam mail 62

Table 3.2 – Sample privacy spam mail 63

Table 3.3 -PCIDSS Goals and Requirements.....75

Table 6.1- Sample spam login alert.....207

Table 6.2 - Sample fraudulent transaction alert.....207

Figure 6.1- Cybersecurity process based on the theory of modalities of control 213

List of Abbreviations

2FA – Two Factor Authentication

BOFIA - Banks and Other Financial institutions Act

BVN - Biometric Verification Number

CBN - Central Bank of Nigeria

CFRN - Constitution of the Federal Republic of Nigeria

CVV - Card verification value

EFCC - Economic and Financial Crimes Commission

EFTPOS - Electronic fund transfer at point of sale

EMV- Europay MasterCard Visa

FITC - Financial Institutions Training Centre

LFN - Laws of the Federation of Nigeria

NAPTIP - National Agency for the Prohibition of Trafficking in Persons

NCC - Nigeria Communications Commission

NDIC- Nigeria Deposit Insurance Corporation

NDLEA - National Drug Law Enforcement Agency

NEFF - Nigeria Electronic Fraud Forum

NIDB - National Identity Database

NIMC - Nigeria Identity Management Commission

NIN - National Identity Number

NNIMC - Nigeria Identity Management Commission Act

NWLR - Nigerian Weekly Law Report

ONSA- Office of National Security Adviser

OTP - One Time password

PCIDSS – Payment Card Industry Data Security Standards

PIN - Personal identification number

POS - Point of Sale

SCN - Supreme Court of Nigeria

SCNJ - Supreme Court of Nigeria Judgements

SIM - Subscriber Identity Module

Chapter One

Introduction

The emergence of the digital economy has generated much debate about cybersecurity. This is more so in Nigeria with the increasing adoption of electronic means of payment. E-payment systems are expected to facilitate the development of e-commerce through a range of technology driven payment instruments and services. They are also expected to improve banking and payment services and ultimately facilitate Nigeria's integration into the digital market place. Therefore, the migration of consumers to e-payment systems is backed by active government policies. However, developments in cybersecurity laws have not corresponded with government's policies to promote the digital economy and in spite of its relative nascence, e-payments are already being exploited by criminals.

Increased criminal activities are particularly significant because Nigeria already has one of the highest records of internet crimes in the world.[1] The high record of criminality has been attributed to a number of factors including lack of legislation on cybercrimes and lack of regulation in the general area of cybersecurity. As a basis for understanding the challenges of developing and implementing cybersecurity laws in Nigeria, this research examines the legal and regulatory responses to identity-related cybercrimes in e-payment systems. Where there have been no responses, the analyses in the thesis examines the reasons which account for lack of responses.

The thesis starts with a general overview of law and regulation of the e-payment industry in Nigeria. It follows with the analysis of the cybercrime threats to e-payment systems. It then examines the legal and regulatory structures put in place to control cybercrime in Nigeria. The thesis follows with the analysis of the theories of regulation of cyberspace and how these aid the understanding of the relevance and primacy of legal regulation. It concludes with recommendations for achieving cybersecurity consistent with the legal, enforcement and regulatory environment in Nigeria.

This chapter sets out the broad framework for the thesis. It describes the central thesis of the research and its originality and contribution to knowledge. It also sets out the

[1] See eg Federal Bureau of Intelligence Internet Crime Complaint Centre, '2013 Internet Crime Report' <https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf> accessed 01/06/2015.

principal research questions sought to be answered and a synopsis of the chapters in the thesis. The chapter concludes with a description of the methodology employed to answer the questions, the data analysis technique, how ethical issues were addressed, and the limitations of this research.

1.1 Central Thesis and Contribution to Knowledge

It is argued in this thesis that innovations in payment systems have positive and negative implications for the development of the digital economy. Lack of legal regulation will promote the negative effects of cybercrime and encroach on user trust and confidence. Conversely, legal regulation of security and privacy standards in e-payment systems will control the negative effects of cybercrimes and increase user confidence and trust in electronic transactions. However, criminal laws which have been the main focus of policy in Nigeria provide scant protection against the threats of cybercrimes. It is argued that rather than the criminal law, law and policy makers should focus on an amalgam of laws particularly those that boost data protection and engender trust in electronic transactions. As preventive measures, these laws offer better protection than the reactive criminal law.

Apart from the literature which implicates Nigeria in pervasiveness of cybercrimes, there is a relative paucity of literature on cybercrimes and cybersecurity in Nigeria. In addition, the existing literature is devoted to advocating an update of the criminal law to accommodate new forms of online offending. Little is thus understood on why criminal laws have not been passed or their limitations in dealing with cybercrimes. Different to other research, this thesis goes beyond the rhetoric of criminal legislation. Using e-payment systems as a case study and following the notion that law cannot be examined in a vacuum, the thesis investigates the legal, social and cultural constraints to implementing cybersecurity in Nigeria. It proposes that by understanding these issues, we may better develop a proposal that meets the exigencies and idiosyncrasies of the social and legal environment. The research is therefore original in two distinct ways. One, it advances the literature by providing explanations based on empirical study, on the reasons underpinning the current responses (or lack of it) to cybercrimes in Nigeria. Two, based on the understanding of the socio-legal environment, it proposes a regulatory model for cybersecurity in Nigeria. The findings made by the research will enhance the development of the digital economy in Nigeria by negotiating an appropriate approach to controlling theft and fraud online. It will also have far-reaching implications for controlling other cyber-related crimes such as money-laundering and terrorist financing.

1.2 Principal Research Questions

The objective of the research is summed up in a research question as follows; to what extent has the Nigerian law evolved to meet the challenges of cybersecurity in electronic transactions? In order to place the investigation within the context of e-payment systems, this thesis will also answer the following specific questions; what are e-payment systems and what role do they play in development and governance in Nigeria? How do cybercrimes threaten e-payment systems and how has industry and policy responded to the threats? To what extent has the criminal law responded to the threats of cybercrimes and what reasons account for the response(s) or lack of it? How does the understanding of data protection regimes aid the prevention of identity related cybercrimes and to what extent has the Nigerian law integrated data protection standards? How do theories of cyberspace regulation aid the understanding of the limits of private ordering systems and self-regulation in the context of controlling identity-related crimes in e-payment systems? To aid the development of the electronic economy and considering the context of the Nigerian society and nature of cybercrimes, how should the law best address the challenges of identity related cybercrimes in e-payment systems?

1.3 Chapter Structure and Synopsis

To address the research questions, the thesis is divided into seven further chapters as follows:

Chapter Two – Legal and Institutional Frameworks for E-payment Systems in Nigeria

Chapter two provides an important background context for the thesis in three ways. First, it provides relevant background information on the Nigerian legal system including the constitutional framework and law making process. Second, it highlights the development of e-payment systems in Nigeria and demonstrates how new payment instruments, channels and institutions pose new challenges for traditional banking and financial regulation. Third, the chapter examines the significance of e-payments to economic growth, development and governance in Nigeria.

Chapter Three – Cybercrime Threats to E-payment Systems

Chapter three also sets an important analytical background for the examination of law and policy on the control of identity-related cybercrimes in Nigeria. Against the background of data collected during the fieldwork, the chapter examines different forms of cybercrimes that threaten e-payment systems, services, institutions and users. The chapter begins by charting the development of cybercrimes in Nigeria. It then evaluates the re-emergence of

cyber-fraud as a problem in the face of new e-payment systems. The chapter considers in particular the threats posed by criminal activities such as hacking, phishing and spamming, and identity theft and fraud. It also explicates the position of service provider organisations, particularly telecommunications and financial and non-financial organisations, as threat vectors. In establishing the links between data breaches and identity theft and fraud, the chapter examines the notion of identity, its digital dimensions and the criminal use of identity information in e-payment systems in Nigeria. The chapter concludes with the consideration of the solutions offered to resolve threats to identity information. It examines in particular technologically based solutions such as authentication protocols and encryption, the Payment card Industry Data Security Standards (PCIDSS) and the various regulations and guidelines provided by the Central Bank of Nigeria to ensure consumer protection and deter identity theft and fraud.

Chapter Four –Criminal Law Responses to Identity Related Cybercrimes

Chapter four evaluates the responses of the criminal law to cybercrimes generally and identity related crimes in particular. The chapter examines the extent to which the threats identified in chapter three have been criminalised. It evaluates the position of extant criminal legislation on hacking, phishing, identity theft and fraud relative to traditional crimes such as burglary, criminal trespass, impersonation and fraud. Based on the examination of the relevant provisions of the proposed law on cybercrime in Nigeria, the Cybercrime Bill 2014, and its juxtaposition with those of the UK Computer Misuse Act 1990, the analysis identifies gaps in the Nigerian criminal law. Finally, using the empirical data and the literature, the chapter provides some understandings of the challenges and limits of criminal legislation to combat cybercrime. It examines in particular how perceptions of the crime by the society, law enforcement agents and even lawmakers may affect the effectiveness of a cybercrime law.

Chapter five- Regulation of Data Processing in Nigeria

Chapter five examines alternative regulatory approaches implicating service provider organisations in the protection of consumer information which are susceptible to criminal exploitation. The chapter begins by identifying the links between privacy and e-payment systems. It then referenced the literature in distinguishing between the concepts of privacy and data protection. The analysis in the chapter proceeds with the examination of the state of the Nigerian law on regulation of data processing. In particular, the chapter evaluates different regulatory guidelines developed by the telecommunication and financial sectors on

data protection. Using the UK/EU Data Protection law as the main comparative reference, the chapter concludes with the examination of the provisions of a draft Nigerian data protection law which is modelled closely to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. It examines the scope of the proposed law and interpretational and conceptual challenges which it may pose considering the nature of the internet and in the context of mandating organisations to protect personal information.

Chapter Six – Theories of Regulation in Cyberspace

In order to underscore the limits of technology and industry private ordering systems in the control of identity-related cybercrimes, chapter six examines the theories of regulation in cyberspace. The chapter sets out the respective theories of cyberspace regulation and evaluates the cyber-libertarian and cyber-paternalists concepts of regulation. Having critiqued the different regulatory approaches advanced by the two schools of thought, the chapter argues that Lessig's alternative theoretical framework of modalities of regulation is useful for addressing the problems of identity theft and fraud in e-payment systems. The chapter tests the validity of this position by demonstrating how technology, industry and norms fail to regulate effectively unless they are backed by the force of law.

Chapter Seven – A Proposal for Cybersecurity in E-payment Systems in Nigeria

Chapter seven follows up on chapter six and argues that an approach promoting law as the primary source of regulatory rules should apply in the particular context of the Nigerian system. In order to provide further support for this position, the chapter summarises and reviews the main findings and arguments from the empirical data and the literature. It argues in particular that for cybersecurity laws to be effective, there must also be an understanding of how different laws function in different socio-cultural and legal and regulatory contexts. In this respect, the chapter identifies the systemic problems of implementing and enforcing the cybercrime law in Nigeria. It also highlights the general ineffectiveness of the criminal law in controlling cybercrime at national and international levels. The chapter therefore recommends that policy should focus on preventive non-criminal legislation rather than cybercrime laws which are essentially reactive. Based on the findings from the empirical data, the chapter concludes with specific recommendations which should be implemented to achieve cybersecurity in Nigeria.

Chapter Eight –Conclusion of Central Thesis

Chapter Eight concludes the thesis. It re-examines the research questions and identifies the broader applicability of the research findings.

1.4 Research Methodology

The research takes an exploratory approach to developing an understanding of the control of identity related cybercrimes in e-payment systems in Nigeria. A qualitative methodology is found to be more appropriate in addressing the research questions and the thesis employs both documentary and empirical methods of research.

1.4.1 Documentary Research

Documentary research involves a review of existing literature to provide the background for a theoretical analysis of the questions posed by the research. In this regard, primary sources such as statutes and case laws are examined. Carefully selected secondary sources of information including texts, journal articles, records of legislative proceedings and relevant grey literature are also examined. Notably, documentary analysis provide important insights into the subject or phenomenon being studied and aid the understanding of existing theories and development of new ones. As Webley noted, the importance of documentary analysis in legal research is underscored by the fact that documents provide evidence of directions. They also provide evidence of legislative intent and provide understandings of perceived shortcomings or best practices in the legal system as well proposing an agenda for change.[2] More crucially, where the research involves empirical work, textual data may be used to support observational or interview findings.[3]

While this research is not essentially comparative, the thesis involves some comparative analysis. The documentary research draws on the literature pertaining to cybercrimes and cybersecurity in other jurisdictions particularly the UK. Generally, comparative materials can serve as an illustration or constitute persuasive authorities, they can be supportive of an argument and they help to elucidate existing rules of law to test its soundness or otherwise.[4] Therefore, the comparative perspectives in this research stems from its usefulness in enabling the thesis to examine what is right or wrong with the legal process or system in Nigeria based on available materials and experiences in the UK. The UK is particularly

---

[2] Lisa Webley, 'Qualitative Approaches to Empirical Legal Research' in Peter Cane and Herbert 'M. Kritzer, *The Oxford Handbook of Empirical Legal Research* (OUP 2010) 11.
[3] Kathy Charmaz, *Constructing Grounded Theory* (2nd edn, SAGE 2014) 48.
[4] Charles Proctor, *Mann on the Legal Aspects of Money* (6th edn, OUP 2006).

relevant because Nigeria shares a common law origin with the UK and still references English laws, cases and practices in her legislative and judicial systems. Hence, cases from the UK are said to have 'persuasive' authorities on the Nigerian courts.

It is however important to state that the thesis did contain an isolated review of the literature in the sense of summarising the findings in the literature in a single chapter. The approach taken here is to integrate the review into the body of the thesis and to summarise the literature throughout the whole project. This approach is followed because it provides an avenue not only to summarise the existing literature but also to synthesise the literature with the analysis and context of the research.

1.4.2 Empirical Study

The purpose of the empirical work is to provide explanations and insights into the challenges of achieving cybersecurity from practical perspectives of practitioners and experts in the area. It is particularly useful to this research because cybersecurity is a new and emerging area in Nigeria and the literature is typically and expectedly scant. The empirical data therefore fills the gap by providing additional and alternative means of identifying and understanding the problems. The empirical work is also useful for theorising and therefore generalising the research findings. According to Creswell, an appropriate methodology must capture the philosophical assumptions of the researcher including the ontological and epistemological perspectives underpinning the research. [5] Qualitative research methodologies are therefore inductive, emerging, and shaped by the researcher's experience in collecting the data.[6] Consequently, good qualitative data are more likely to lead to unanticipated findings which help researchers to get beyond initial conceptions and to generate or revise conceptual frameworks.[7]

1.4.2.1 Choice of Participants

With respect to the identification and choice of participants, a purposive sampling method was adopted. In a purposive sampling, the researcher's priority is the relevance of the selected sample group and the contributions of their account of reality to the task of answering the research questions.[8] The use of this form of sampling to generate qualitative data is therefore founded on the need to examine from practical perspectives the challenges

---

[5] John W Creswell, *Qualitative Inquiry and Research Design Choosing Among Five Approaches* (Sage 2013) 22-41.
[6] ibid.
[7] Matthew Miles and Michael Hubberman, *Qualitative Data Analysis: An Expanded Sourcebook* (Sage 1994) 1.
[8] S Sarantakos, *Social Research* (2nd edn, Palgrave 2005) 152.

posed by cybercrimes. This approach to qualitative inquiry is important to the objective analysis of the subject of the research and the validity of the conclusions reached by the thesis.

Following the above, participants in the fieldwork were selected from law enforcement agencies engaged in cybercrime investigations and prosecution (hereinafter law enforcement), officials of banks and non-bank organisations providing e-payment services (hereinafter payment service providers), and regulators of the payment and financial industry (hereinafter regulators). Other participants include lawmakers in the Nigerian National Assembly (hereinafter lawmakers), government agencies engaged in policy formulations and legal drafting (hereinafter policy makers) and information security experts (hereinafter IT security experts). A total of 21 interviews were conducted. These include 9 payment service providers, 3 policymakers, 4 lawmakers, 2 representatives of regulatory bodies and 3 IT security experts. 19 interviews were eventually analysed as two participants withdrew their participation.

It is important to mention that while the validity of a qualitative inquiry is not necessarily linked to a large number of participants,[9] the relatively small number of interview participants in this research reflects the dearth of expertise in the area of cybercrimes and cybersecurity in Nigeria. On the part of payment service providers, the newness of the services, and the inclination of payment service providers to engage third party information security organisations, perhaps explains the relative lack of expertise. However, expertise is equally lacking among law enforcement agencies, policy makers and lawmakers. For example, some central policy making authorities have virtually no staff and law enforcement is made up of very small circle of cybercrime investigators or "experts". Also, because of the high rate of turn-over in the legislative houses, most lawmakers have had no opportunity and/or experience of participating in any debates on cybercrime/cybersecurity laws. Therefore, selection had to be made among the principal officials of the legislative houses based on availability and willingness to participate in the interviews, but most importantly, based on their access to archived documents and legislative records. These participants were identified through referrals within the legislative house itself.

1.4.2.2 Form of Interviews

The empirical work was conducted through qualitative interviews and all interviews took place from April to July 2013. The choice of qualitative interviews is based on the role it

[9] see Charmaz (n 3) 105-108; see also notes on generalizability of Findings below.

plays in "interpretive inquiry".[10] For example, qualitative interviews allow the researcher access to otherwise inaccessible areas such as people's subjective experiences and attitudes.[11] The interviews can also be used to understand the meanings which people attach to both their own actions and those of other people.[12] They can therefore expand the horizons of a studied phenomenon and encompass both the 'how' and the 'why' of the inquiry. As noted by Rubin and Rubin, 'If what you want to find out cannot be answered simply or briefly, if you anticipate that you may need to ask people to explain their answers or give examples or describe their experiences, then you rely on in-depth interviews'.[13] Based on these elements, qualitative interviews was found to be a more appropriate method of eliciting comprehensive responses on issues such as the scope of fraudulent electronic payment activities, the nature of the responses to the activities, and the limits and effectiveness of such responses as well as reasons for legal responses or lack of it.

Furthermore, semi-structured interviews are used in preference to loosely structured interviews because when viewed from the perspective that qualitative interviews are guided conversations, they tend to be more useful in generating data.[14] Semi-structured interviews enable the researcher to have some set questions while the majority of the questions will then be open-ended rather than closed.[15] This approach is useful in a number of ways. It enables the questions which are of interest to the researcher to be covered while also allowing room for the views of the interviewee to be freely expressed and incorporated. It also enables the researcher to achieve a balance in the interviewer/interviewee relationship because semi-structured interviews minimise status differences between interviewer and respondent and can avoid the hierarchical pitfall.[16] Finally, semi-structured interviews enable greater openness and insight, which can facilitate a wide range of responses, leading to fuller and richer data.[17] In the context of this research therefore, semi-structured interviews assisted the researcher to strike a balance between eliciting relevant information

---

[10] Kathy Charmaz, *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis* (SAGE 2006) 25.
[11] Anssi Rerakyla and Johanna Ruusuvuori, 'Analysing Talk and Text' in Norman K Denzin and Yvonna S. Lincoln (eds) *The SAGE Handbook of Qualitative Research* (4th edn, SAGE 2011) 529.
[12] Webley (n 2) 4-9.
[13] Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing: The Art of Hearing Data* (2nd edn, SAGE 2005) 2-3.
[14] ibid 3.
[15] Webley (n 2) 9.
[16] Uwe Flick, *An Introduction to Qualitative Research* (3rd edn, SAGE 2006).
[17] Punch K F, *Introduction to Social Research: Quantitative and Qualitative Approaches* (2nd edn, SAGE 2005).

from law enforcement agents and industry regulators who were more receptive to fairly long interviews or more open questions and from representatives of payment service providers who were more reticent because of the constraints of time and the confidential nature of financial services.

1.4.2.3 Conduct of Interviews

Whether identified prior to commencement of fieldwork or subsequently through referrals, all participants were contacted by letters inviting them to participate in the interviews. A Participant's information sheet setting out the expectations and procedures to be followed during the interviews was annexed to the interview letters. Most participants communicated their willingness to participate in the interviews by contacting the researcher through the telephone or e-mails. All the interviews were carried out in Nigeria and were conducted in the workplace or offices of the participants. The participants were professionals and experts in their respective fields and the interviews were conducted in an atmosphere of mutual respect between the researcher and the participants.

The general format of the interview questions contained the main questions sought to be covered during the interviews. Following the need to elicit as much information as possible, the questions were framed in open-ended language. Also, to avoid pre-empting answers from the participants, the format contained no leading questions. However, the profession and area of expertise of the participants, as well as responses to the initial questions often require that subsequent questions be modified or additional questions asked to elicit meaningful and comprehensive information. In such cases, the researcher asks follow up questions intended to generate specific responses. This approach is consistent with the form of qualitative interviews which embed flexibility and openness.

To re-establish participants' voluntary participation, they were requested to sign a 'consent form' before the commencement of the interview.[18] All responses to interview questions were handwritten and no audio or visual recordings were made. However, note-taking posed some challenges particularly in cases where the participants speak very fast and in fairly long interviews. Although longer interviews invariably generate a wide range of useful data, it also often means it is difficult to maintain a steady and unbroken speed of note-taking. Since the researcher was aware that the target participants may be opposed to the recording of the interviews in the first place, requests were only made for participants to either repeat their responses or to speak slowly rather than a request to switch to recording the responses.

[18] See notes on research ethics below.

Although, ultimately, the note-taking means the interview text sometimes trails off and when repeated, the impact or meaning of certain statements is lost or reduced, the note-taking process also aided the richness of the information. For example, because they were not being recorded, participants appear more confident to give "sensitive" or "off the record" information.[19] Notably, most participants still gave permission for comments made "off the record" to be written down and used by the researcher provided the participants could not be identified.[20] Taking handwritten notes therefore presumably put the participants more at ease and willing to disclose relevant and important information.

1.5 Research Ethics- Informed Consent and Data Protection

Consistent with the University's code of ethical conduct, ethical approval was sought and obtained before the commencement of the fieldwork.[21] In giving the ethical approval, the ethics committee evaluated the research questions, the letters proposed to be sent to the participants, and the participant's information sheet as well as the participants consent form.

Before and during the interviews, all participants were informed about the process of the interviews including the fact that participation was completely voluntary. Participants were above the age of 18 and did not belong to any group of vulnerable individuals. They were all therefore able to and did give their consent to the interviews by signing the declaration on the participants' consent form.

The research did not identify any risk of mental or psychological distress to any of the participants. There were no anticipated or actual conflicts of personal, financial or professional interests. The participants were professionals and offered information voluntarily without any financial or other inducements. They were informed that they could request for and will be sent transcripts of their respective interviews.

All personal and identifying information collected during the interviews were kept in accordance with the Data protection law and the University Of Leeds Code Of Conduct on Data Protection. Interview transcripts in the form of typed and handwritten notes were kept

---

[19] One example of "off the record" information is one participant's observation that Nigerian lawmakers needed to be 'lobbied' in the form of monetary and other incentives to pass a bill into law. When asked to clarify this notion of lobbying, a lawmaker also answered, 'what do you mean we are being lobbied? …. 'That's not true… it's extremely damaging… people shouldn't talk like that…'

[20] These assurances were given verbally although they were already stated in the accompanying explanatory note.

[21] Application for ethical review was made using the University of Leeds Research Ethics Committee Application Form Version 11.

safe in a locked cabinet. All data was anonymised and linking information was removed. All data will be destroyed after the completion of this research.

1.6 Data Analysis

The analysis employed systematic coding of the data and used the grounded theory to develop theoretical constructs. Coding in data analysis aids the linking of different segments or instances in the data. It brings fragments of data together to create categories of data having some common property or elements, and allows the differentiation and combination of data and the reflections made about the information.[22] As a tool, coding is meant to be flexible and driven by the researcher's insights.[23] It is therefore a heuristic device used to link the data to ideas and concepts rather than an end in itself. It is generally intended to exploit the directional, critical, and analytical dimensions of the data.[24] The important analytic work, as Coffey and Atkinson correctly argue, lies in the identification of relevant concepts.[25] Accordingly, Seidel and Kelle assert that, 'codes represent the decisive link between the original 'raw data', that is the textual material such as interview transcripts or field notes, on the one hand and the researcher's theoretical concepts on the other.'[26]

Following the directions above, coding of the interview data in this research was used to assign meanings to words, statements or paragraphs as well as to generate ideas and concepts related to the data. The handwritten interview transcripts were typed and data was manually coded and manipulated to obtain their meanings. Three broad steps were followed to analyse the data. In the first stage, labels or keywords were assigned to characterise the interview data. In the second stage, codes and categories were further analysed for varieties and commonalities. The objective of the second stage was to generate denser set of codes or core categories to which themes could be assigned.[27] A Theme is described as an integrating, rational statement derived from the data that identifies both content and meaning.[28] It is the outcome of coding, categorisation and analytic reflection which

---

[22] Amanda Coffey and Paul Atkinson, *Making Sense of Qualitative Data Complementary Research Strategies* (SAGE 1996) 31.
[23] Corbin J 'Taking an Analytic Journey' in J M Morse (ed), *Developing Grounded Theory* (Walnut Creek Press 2009) 35, 40-41.
[24] Coffey and Atkinson (n 22).
[25] ibid.
[26] Seidel J and Kelle U, 'Different Functions of Coding in the Analysis of Textual Data' in U Kelle (ed), *Computer-aided Qualitative Data Analysis: Theory, Methods and Practice* (Sage 1995) 52 cited in Coffey and Atkinson (n 22) 31.
[27] Pat Bazeley, *Qualitative Data Analysis Practical Strategies* (SAGE 2013) 101-222.
[28] Coffey and Atkinson (n 22) 190.

elucidates the relationship between the coded categories and relevant theoretical conceptions.[29] (*Sample codes annexed as appendix to thesis*)

The third stage of the analysis involved the extrapolation of concepts and ideas from the common themes. This is theoretical coding, which is the interpretative stage of the analysis involving the linking of codes or core categories to the literature in order to understand the theoretical implications of the data. As Coffey and Atkinson argue, although theories are intrinsic in the research process itself, and often inform the coding process, however, since generalisation of ideas is not dependent on the data alone, careful examination of codes can also help to generate formal substantive theoretical ideas.[30] Notably, when theoretical constructs develop later in the research, and after data collection and analysis, as in the case of this research, they are said to be grounded in the data. Grounded theory is defined as the discovery of theory from data systematically obtained and analysed in social research.[31]

It is important to note here that because qualitative research involves personal engagement with data collection, interpretation and reporting, it is often perceived as subjective. It is therefore the responsibility of the researcher when coding the data, as with when selecting the participants,[32] to eliminate researcher opinions or prior concepts which may bias or prejudice the analysis. In this research, data was treated uniformly and consistently either by ruling out alternative explanations for the interpretation given by the researcher or by finding sources independent of the data, which support the interpretation. Also, in order not to stereotype the data, the researcher searched for variability and data which did not fit prior expectations. For example, throughout the thesis, policy documents, reports and statistics as well as comparative analysis from other jurisdictions were used to underline the correctness of certain extrapolations made from the data or to rule out alternative explanations for the conclusions drawn.[33]

Furthermore, since eliminating researcher bias also involves the use of appropriate data analysis method, the grounded theory approach used in this research aided the researcher to deal with and overcome conceptions made prior to data collection and analysis. As already

---

[29] Saldana J, *The Coding Manual for Qualitative Researchers* (SAGE 2009) 13 cited in Bazeley (n 27) 190-191.
[30] Coffey and Atkinson (n 22) 141-153.
[31] Barney G Glaser and Anslem L Strauss, *The Discovery of Grounded Theory* (Weidenfield and Nicolson 1967) 1, see also Cathy Urquhart, *Grounded Theory for Qualitative Research* (SAGE 2013) 4.
[32] See notes on generalizability of findings below.
[33] See e.g. notes in 4.2.3.1 Access without Authority (Basic Hacking Offence) 97 particularly at 98-103.

implied above, grounded theory refers to both the process of coding itself and to the theory generated from the data. As a process of coding, the role of the theory is to highlight the fact that irrespective of the researcher's preconceived notions, the data is bound to reveal accounts of the phenomenon which cannot be formulated or conceived independently of the data. Therefore, while grounded theory does not presuppose that the researcher has no preconceived notions of theories or the literature, it overrides such preconceptions because it ensures that the researcher keeps an open mind on the findings which may emerge from the data, and ensures the researcher's formulation of theories is based on the findings.[34]

As a final point in this section, it is important to state that similar to the literature review, findings from the empirical research are integrated into the entire body of the thesis rather than being presented as a separate chapter. This approach provides cohesion and better contextual understanding of the data than would a dedicated chapter which may produce fragmented and disjointed data sets.

1.7 Generalisability of Findings

Generalisation in qualitative research is often contested because of the context specific nature of the research and the involvement of the subjective experience of the researcher.[35] However, in the preponderance of the literature, it is also agreed that the notion of generalisability in qualitative research is to be understood in terms of extrapolations and interpretations which may form the basis for understanding situations and cases other than those directly studied.[36] In this respect, qualitative researchers may lay claim to external or internal generalisation of their findings. Internal generalizability refers to generalising from cases and settings directly or actually studied to those not studied but which are within the same setting.[37] The validity of internal generalizability depends on whether the sample directly studied is representative of the population within that setting.[38] External generalisation involves generalising to contexts or cases beyond the setting studied.

---

[34] See Urquarth (n 31).
[35] See e.g. Martyn Hammersley, *Questioning Qualitative Inquiry: Critical Essays* (Sage 2008); see also David Wainwright, 'Can Qulaitative Research be Qualitative, Critical and Valid' (1997) 3(2) The Qualitatve Report.
[36] See e.g. Joseph A Maxwell and Margaret Chmiel, 'Generalisation in and From Qualitative Analysis' in Uwe Flick, (ed) *The Sage Handbook of Qualitative Data Analysis* (Sage 2014), 540; see also Mike Metcalfe, Generalisation Learning Across Epitemologies' (2005) 6(1) Forum: Qualitative Social Research available <http://www.qualitative-research.net/index.php/fqs/article/view/525/1136?ref=driverlayer.com/image> accessed 05/11/2015.
[37] Joseph A Maxwell, 'Understanding and Validity in Qualitative Research' (1992) 62(3) Havard Educational Review 279, 293.
[38] ibid 284.

Although, internal generalizability is often regarded as a more legitimate claim by qualitative researchers, this is not to say that claims to external generalisation cannot be made. As Becker argues, generalisation in qualitative research usually takes place through the development of theories which make sense not only of the particular case or phenomenon studied but also shows how the same process can lead to different results in different situations.[39] As Johnson and Christensen also correctly observe, a well-developed theory explains how something operates in general and enables one to move beyond the findings of any single research.[40]

In this thesis, an important claim made to generalizability is the formulation of a theory which underlines the impacts of socio-cultural and political and institutional factors to the development of cybersecurity laws. This theory suggests that if law and policy take into account socio-cultural and political and institutional contexts of a society, legal and regulatory responses to cybercrimes can become more effective. Therefore, even in the globalised contexts of cybercrime and cybersecurity, the development and effectiveness of laws will be determined by the socio-political ethos of respective jurisdictions. In effect, while the research avoids exaggerated claims to external generalizability in terms of the fact that its findings are immediately transposable to a different jurisdiction, the theory it has generated make the findings relevant for understanding the relevance of socio-cultural and political contexts in cybersecurity discourse and solutions. These contexts might be similar or diverse but they are present and should be taken into account.

As noted above, internal generalisation is far more important in qualitative research because it underpins the validity of inferences drawn from the sample or case directly studied. Therefore, as this research investigates the legal and regulatory responses to identity–related cybercrimes, the purposive sampling approach already described above was used to identify participants whose accounts are crucial to the case study. [41] This sampling method takes into account the knowledge, experience and expertise of the sample population to the investigation. To illustrate, participants were chosen from service provider organisations because they are adequately positioned to give more accurate information about the nature of cybercrimes that threaten e-payment systems and to understand the responses which have been developed and how law and policy may otherwise respond to counter the threats. Also,

---

[39] Howard Becker, 'Generalising from Case Studies' in Elliot W Eisner and Alan Peshkin (eds), *Qualitative Inquiry in Education: The Continuing Debate* (New York Teachers College Press) 240.
[40] Johnson B and Christensen L, Educational Research: *Quantitative, Qualitative, and Mixed Approaches, Research Edition* (2nd edn Pearson), 19.
[41] See notes in 1.4.2.1 Choice of Participants above.

lawmakers, law-enforcement agents and security experts as well as regulatory agencies were chosen for their relevance in giving diverse and varied accounts of cybercrime and the reasons underlying legal responses or lack of responses. In terms of its internal generalizability therefore, the sample used in this research is sufficiently representative of the population of available service providers and experts in the area of cybercrime and cybersecurity in Nigeria.[42] As Miles and Hubberman aptly point out, although the validity of results depends on their internal generalizability to the particular case or setting being studied, it is impossible to study 'everyone everywhere doing everything, even within a single case'.[43] However, even if this was possible, it is arguable that not all possible accounts of individuals, phenomena or institutions are equally useful, credible, or legitimate.[44] In view of this position, the extrapolations made from the account of the participants in this research are as applicable to the narrow area of identity-related cybercrimes in e-payments as they are to the broader area of cybercrime and cybersecurity.

1.8 Limitations of the Research

This research represents one of the most comprehensive attempts to understand the problems of cybersecurity in Nigeria. It sets the tone for further inquiry, questions and debates on the approach to regulating and controlling the growing problem of cybercrimes. However, it suffers from two limitations. The first is that because the area of the law is relatively new, literature and statistics are sparse. This means reliance had to placed almost exclusively on foreign literature and the views and opinions of few experts in the field of cybersecurity in Nigeria. The second, closely associated with the first is the dearth of expertise in the area of cybercrimes and cybersecurity. Given that only few people are knowledgeable in the area, the number of participants in the interviews is further limited to the accessible individuals who could give expert and authoritative information and opinions on the subject. This may have limited the perspectives from which the problems could be understood. However, this deficit also provides the background for further research particularly quantitative research into areas of privacy behaviour and societal perceptions of cybercrimes.

---

[42] ibid.
[43] Mathew B Miles and A Micheal Hubberman, *Qualitative, Qualitative Data Analysis: Sourcebook of New Methods* (Sage 1984) 36.
[44] see Maxwell (n 37) 282-283.

Chapter Two

Legal and Institutional Frameworks for E-payment Systems in Nigeria

Introduction

E-payments are important for development and are essential to leverage the advantages of e-commerce. Since the late 1990s, government policy in Nigeria has focused on reforming the payment systems and the promotion of e-payment systems became a top policy agenda for the government. However, the ensuing migration to e-payment systems has implications for the financial industry, and the users of payment services as well as for law and policy. E-payments implicated banks, other financial institutions, telecommunication providers and other organisations in service provision, and payment facilitation and transmission. Also, while the system enhanced interoperability, convergence and competition in the payment industry, they aggravate the risks of cyber-intrusions, and other computer-related crimes which raise the threats of identity crimes in fund transfer systems.

This chapter provides an overview of e-payment systems in Nigeria. The chapter is divided into two parts. As a useful reference for later discussion in the thesis, the first part gives some background information on the Nigerian legal system. It discusses the sources of Nigerian laws and shows its links with English law. It also highlights the constitutional arrangement and the legislative and judicial processes in Nigeria. The second part examines the development of e-payment systems in Nigeria. It analyses the impacts of respective payment instruments and the institutional arrangements for payment systems on users and consumers. It also examines the legal status of e-payments relative to cash. The chapter concludes with an examination of the major justifications for e-payments in Nigeria and its advantages for e-commerce as well its implications for new forms of crimes.

2.1 PART I - An Introduction to the Nigerian Legal System

2.1.1 Sources of Law

Historically, Nigerian law developed from English law. British colonisation of Nigeria effectively started with the annexation of Lagos in 1861. In 1900, Northern Nigeria became the protectorate of the British. Southern Nigeria, together with the colony of Lagos was also declared the colony and Protectorate of the British in 1906. Upon the commencement of

colonial rule, English law was introduced, first into the colony of Lagos and subsequently into the rest of Nigeria.[1] These laws became applicable and the courts were empowered to enforce the common law of England, the doctrines of equity and statutes of general application in force as at January 1, 1900.[2] Customary laws and practices of the indigenous people were also preserved and they were applicable provided that they were not repugnant to natural justice, equity and good conscience, and were not incompatible with statute.[3] In 1914, both the Northern and Southern protectorates were amalgamated and became the country known today as Nigeria. However, owing to religious, political and geographical diversity, the amalgamated entities continued to be administered separately.[4] A legislative council constituted in 1862 (called the Lagos Legislative Council) made laws for the colony of Lagos and Southern Nigeria while in the north; laws were made by the Governor-General of Nigeria. Even today, this dichotomy continued to impact on the legal and political landscape. For example, in the North, the Penal Code which is based on criminal justice according to Islamic laws is used.[5] In the Southern part of the country, sharia system is not recognised and the Criminal Code Act is the major legislation defining criminal conduct and punishment.[6]

2.1.2 Constitutional Framework

Nigeria became independent in 1960 and became a Republic in 1963. The country had operated a number of constitutions both during colonial era and post-colonial rule. Earlier colonial constitutions operated a unitary system of government,[7] while latter constitutions promoted federalism which was eventually inherited and operated since independence.[8] Under the Constitutions of 1960 and 1963 respectively, Nigeria was divided into three Regions. These regions had extensive powers under the constitutions relative to the federal government. The regions had separate constitutions and coat of arms. They also had residual powers to legislate on matters which were not allocated to either the federal government or

---

[1] See Supreme Court Ordinance No 11 of 1863, Ordinance of the Settlement of Lagos 1862-1870 compiled by A Montague (1874).
[2] See Supreme Court Proclamation No 8 of 1900.
[3] See Supreme Court Ordinance No 6 of 1914 Nigeria Ordinance, Orders and Regulations (1914).
[4]See National Assembly, 'History of the Nigerian Senate' <http://www.nassnig.org/nass/history.php> accessed 19/05/2015.
[5] See Penal Code Act Cap P3 Laws of the Federation of Nigeria (LFN) 2004 (hereafterin Penal Code Act).
[6] See Criminal Code Act cap C38 LFN 2004 (hereinafter Criminal Code Act) The Criminal Code is mostly used for the analysis in the thesis.
[7] For example Clifford Constitution 1922 and Richards Constitution 1946.
[8] See McPerson Constitution 1951; see also Lyttleton Constitution 1954.

the regions. The 1979 constitution reversed this trend, it gave more powers to the Federal government and abolished separate constitutions for the constituent entities.[9] The extant constitution, Constitution of the Federal Republic of Nigeria 1999 (CFRN 1999), substantially reproduced the 1979 constitution by allocating much of the legislative powers to the federal legislature.[10]

2.1.3 The Legislative Process

The CFRN 1999 recognises a multi-tier system of government consisting of the federal, states and local governments.[11] At the federal level, Nigeria operates a bi-cameral legislature with two legislative Houses of the National Assembly. The National Assembly consists of the Senate and the House of Representatives which are the upper and lower legislative houses respectively.[12] This legislative arrangement is replicated in all the states of the federation except that the states operate unicameral legislatures. Legislative powers are defined by the constitution and are divided among the federal and states' legislative authorities depending on whether they fall under the exclusive or the concurrent legislative lists.[13] Only the National Assembly has the powers to make laws with respect to matters on the exclusive legislative list.[14] The National and States' Assemblies have concurrent authority to legislate on matters on the concurrent list.[15] The residual matters are left to only the states. Banks and banking, currency, coinage and legal tender, fingerprints identification and criminal records, and trade and commerce as well as the regulation of wireless, and broadcasting and telecommunications are items under the exclusive legislative list.[16] Since the constitution also expressly provides that the National Assembly has the powers to make laws on matters 'incidental or supplementary' to any of the items on exclusive legislative list,[17] states would be excluded from legislating on such matters. Under the constitution, references to incidental and supplementary matters include references to offences.[18]

---

[9] In 1967, the regions were divided into 12 states, Nigeria is now made up of 36 states and the Federal capital territory, Abuja.
[10] See Section 4(1) – (5) CFRN 1999; see also notes on The Legislative Process below.
[11] See Part I of First Schedule CFRN 1999.
[12] ibid s 4(1).
[13] ibid s 4(2) –(7).
[14] ibid s 4(1) - (5); see also *Attorney-General of the Federation v Attorney-General of Abia State & 35 Ors* (2001) 11 Nigerian Weekly Law Report (NWLR) 689.
[15] See s 4(4)(a), 7(b) CFRN 1999.
[16] ibid items 6, 15, 28, 62, 46, 66 of Pt I, Second sch.
[17] ibid item 68 of Pt 1 second sch.
[18] ibid s 2(a) of Pt 1 second sch.

Law making process at the National Assembly follow constitutionally laid down procedure. A bill may originate from either house of the National Assembly. In order to become law, it must be passed by both Houses of the National Assembly and assented by the President. A bill must be read three times and referred to a committee of the house before it becomes law. The first reading of a bill involves reading the title of the bill in the legislative house where it originated. The bill is not debated or opposed at this stage. The purpose and objectives of the bill are explained and debated at the second reading. If the bill passes second reading, it is referred to a committee of the house which examines the provisions of the bill. The committee may invite presentations and comments on the bill from stakeholders and the public. Following debates at the second reading and subsequent presentations by stakeholders, the provisions of the bill may be amended at this stage. The committee then tenders the bill to the whole house for the third reading. If a bill is passed by two-thirds majority of the house, it is sent to the other house where it follows the same process (first, second, committee stage and third readings). If passed by two-thirds majority of the second House of the National Assembly, it is sent to the executive for presidential assent. If assented by the president, it becomes law otherwise both houses of the National Assembly require a two-third majority to override the presidential veto.[19] Any bill which fails to pass legislative approval within the tenure of a particular National Assembly automatically lapses.

2.1.4 The Judicial System

Nigeria operates a hierarchical structure of courts.[20] The Supreme Court is the court of last resort in all appellate matters.[21] It is followed by the Court of appeal from which all appeals to the Supreme Court originates. Appeal lies from the decisions of Federal and states High courts and customary and sharia courts as well as from martial courts and Tribunals to the Court of Appeal.[22] Although, federal and states high courts are courts of co-ordinate jurisdictions, the federal high court has exclusive jurisdictions over issues relating to banks, banking and other financial institutions, and actions by or against the Central bank of Nigeria relating to coinage, legal tender and fiscal measures.[23]

Under the constitution, the judiciary is independent and neither the National Assembly nor the States' Houses of Assembly can make any laws purporting to oust the jurisdiction of a

---

[19] ibid s 58.
[20] See s 6.
[21] ibid ss 233, 235.
[22] ibid s 240.
[23] ibid s 251(d).

court or a judicial tribunal established by law.[24] The principle of judicial precedent is also recognised by the courts and decisions of courts in England can be cited as authorities in Nigerian courts.

The judicial process in Nigeria has been hindered by a number of factors including inexpedient legislative processes and delays in the judicial process itself. Also, where laws fail to evolve in response to specific developments, courts have been known to engage in 'judicial legislation' violating well-established rule of law that judges/courts must act *jus dicere* (to apply the law) and not *jus dare* (to make the law).[25]

2.2 Part II- Overview of E-Payment Systems in Nigeria

2.2.1 Development of Banking and Payment Systems in Nigeria

Banking business started early in Nigeria, however, the history and development of banking had a chequered history. Lack of confidence in the financial sector was mostly responsible for this position. Since the inception of banking activities, there has been a spate of systemic failures and banks' distress. The first incidence of bank failures occurred in the 1950s when 21 out of the 25 banks then in existence became distressed. In the 1990s, the industry was hit by another wave of distress which led to huge financial losses to both investors and the government. The imminent distress of some banks led to consolidation in the banking industry in 2004. The resultant mergers and takeovers significantly reduced the number of banks in Nigeria from 89 deposit-taking banks to 25 in 2006. Subsequent mergers and acquisition has left the banking industry with 21 banks. However, according to the Central Bank, the primary regulator of the financial industry, banks continued to show 'serious liquidity strain' and had to be given financial support by the apex bank.[26] As a result of the threat of bank failures, customers did not only fear for the safety of their deposits with the banks, they were also unwilling to trust alternative payment instruments provided by bankers.[27]

---

[24] ibid s 8.
[25] See for example *FRN v Fani-Kayode* (2010) 14 Nigerian Weekly Law Report (NWLR) 481, where the court admitted electronically generated evidence in spite of the fact that at that time, the clear letters of the Nigerian Evidence Act did not specifically provide for this.
[26] Sanusi Lamido Sanusi 'Development in the Banking system in Nigeria' <http://www.cenbank.org/documents/speeches.asp> accessed 25/05/2012.
[27] See eg Akudo C Anyanwu, Absalom E Ezugwu, Sale E Abdullahi, 'Electronic Payment Systems (EPS): Facilitating the Development and Adoption in Nigeria' (2012) 9(2) International Journal of Computer Science 1.

As a further result of the above, the economy remained largely cash based. The CBN estimated that in recent years, more than 65 per cent of money in circulation was outside the banking sector and therefore beyond the control of the regulatory authorities.[28] To resolve this problem, the government, through the CBN, introduced a number of policy reforms. Central to the reforms is the development of e-payment systems. The CBN Guidelines on Electronic Banking was introduced in 2003 to regulate the emerging e-banking and e-payment systems. A National Payments Committee was also established by the CBN in 2005. The committee was charged with initiating reforms to increase the diversity and liquidity of payment instruments. The instruments are expected to be adaptable to local circumstances and boost economic development.

Also, in 2005, the CBN formulated the National Payment Systems Vision (NPSV) 2020 to develop e-payment systems specifically. [29] A key objective of the NPSV 2020 is the development of a payment system which is 'nationally utilised and internationally recognised'.[30] In spite of the implementation of different government policies however, success was minimal in terms of the expected migration to e-payment systems.[31] Therefore, in 2011, the CBN launched the 'Cashless Nigeria' project. The main objective of the project is to promote e-payments systems. One of the significant aspects of the cashless policy is the introduction of processing fees for cash transactions.[32] In principle 'processing fees' are actually penalties for using cash instead of alternative e-payment systems. Although, aimed at boosting acceptance of e-payment, the policy is controversial. For example, according to Ledingham;

> ...the Bank's [central or regulatory bank's] role is to facilitate and encourage overall payment system efficiency by continuing to offer currency as just one payment technology amongst several. Alternative payment technologies and

---

[28] See CBN, 'Annual Report and Statement of Account 2009' <http://www.cenbank.org/out/2010/publications/reports/rsd/Annual%20Report%202009.html> accessed 12/06/2012.
[29]See Financial Systems Strategy (FSS) 2020 <http://www.cenbank.org/OUT/SPEECHES/2007/GOVADD18-4-07.PDF> assessed 10/02/2012.
[30] ibid.
[31]See CBN, 'Payment Systems' <http://www.cenbank.org/Paymentsystem/rtgs.asp> accessed 12/05/2012.
[32] See CBN letter titled 'Industry Policy on Retail Cash Collection and Lodgement' (IITP/C/01 Circular BPS/DIR/GEN/CIR/01/003) dated 16th March 2012.

> innovations can be freely allowed within this framework, and users can be allowed to choose freely amongst those competing technologies.[33]

In effect, one could argue that mandatory requirement to use e-payment is inconsistent with the overall function of central banks to promote payment systems. It may even be argued that such a policy is autocratic and unconstitutional.[34] However, even if it is assumed that mandatory use of e-payments is defensible for economic and developmental reasons, it would also be reasonable to assume that policy would put in place measures, legal and otherwise, to safeguard users and consumers of the alternative e-payment systems. It is significant to mention that a proposal to regulate the e-payment industry, the Payment Systems Management Bill 2009 was not passed into law and lapsed with the tenure of the legislative house where it was proposed. Consequently, e-payment services and transactions are presently regulated by industry guidelines issued by the CBN. These are Electronic Banking Regulations 2003 (hereinafter CBN E-banking regulations), Regulatory Framework on Mobile Payment Services in Nigeria 2009 (hereinafter CBN mobile payments regulations), Guidelines on stored Value and Pre-paid Card Issuance and Operation 2010 (hereinafter CBN prepaid/stored value card guidelines), Standards and Guidelines on Automated Teller machines (ATM) Operations in Nigeria 2010 (hereinafter CBN ATM Guidelines), and Guidelines on Point of Sale (POS) Card Acceptance Services 2011 (hereinafter CBN POS Guidelines). The implications and limits of the regulatory guidelines particularly in the multi-stakeholder environment of electronic transactions are considered below.

2.3 Legal Aspects of E-Payments

2.3.1. What is E-Payment (Systems)?

Payment means the exchange of value for goods and services or the discharge of some monetary obligation owed by one person to another.[35] Although, the concept of payment is closely tied to money, money has not always been the instrument of payment. For example, barter was used prior to money. However, currency was the first form of money which derived its legitimacy from the authority of the state, thus it was referred to as legal tender money.[36] Again, however, in spite of its legal status, cash as a form of payment was both

---

[33] Peter Ledingham, 'The Policy Implications of Electronic Payments' (1996) para 18, <http://www.rbnz.govt.nz/speeches/0030141.html> accessed 01/07/2012.
[34] See notes below in 2.3.3 Money as a Social Construct p 28.
[35] Charles Proctor, *Mann on the Legal Aspects of Money* (6th edn, OUP 2006) 66.
[36] ibid.

cumbersome and inconvenient particularly for large and trans-border commercial transactions. Non-cash payments became widely used because of bankers' intermediation and guarantee. Thus non-cash instruments such as cheques, bills of exchange and later credit cards came to be used extensively for personal and business payments. It is to be noted that while cash may be transferred anonymously and without the intervention of intermediaries, intermediaries are indispensable to non-cash-payments. These payments are therefore effected by systemic processes and operational arrangements which enable the transfer of monetary value from payer to payee. These systemic processes are commonly referred to as payment systems. [37]

Payment systems are generally defined as composite systems consisting of rules, standards and instruments used to exchange financial value between parties discharging an obligation.[38] They consist of institutions, the various forms of money, and the channels for communicating payment instructions,[39] as well as the organisational, institutional and legal and regulatory frameworks which make up the system. [40] Accordingly, Geva defines a payment system as "…any machinery facilitating the transmission of money in the payment of a debt, which enables the debtor to avoid the physical transportation of money and its physical delivery from the payer to the payee."[41] Electronic payments are distinct in two ways. One, they utilise electronic network systems. Two, they are achieved without face-to-face interaction. They have therefore been defined as payments initiated, processed and received electronically. [42] In the context of e-commerce, e-payment systems enable the exchange of value electronically for goods, services or information. Therefore, the European Central Bank defined e-payments more aptly as payments made over the internet using remote payment card transactions, online banking systems or e-payment providers with which the consumer has set up individual accounts.[43] This definition clearly implicates the

---

[37] Ludwig Gramlich, 'Electronic Payments and Electronic Money-Some General Remarks on Factual and Legal Developments' (2008) 2 Masaryk UJL & Tech 39.
[38] Austin Briggs and Laurence Brooks, 'Electronic Payment Systems Development in a Developing Country: The Role of Institutional Arrangements' (2011) 49 EJISDC 3, 1.
[39] C.E.V Borio and P. Van den Bergh, 'The Nature and Management of Payment System Risks: An International Perspective' (BIS Economic Papers No 36 1999).
[40] Briggs and Brooks (n 38) 16.
[41]Benjamin Geva, 'The Concept of Payment Mechanism' (1986) 24(1) Osgoode Hall LJ 1, 4.
[42] David B. Humphrey, Lawrence B. Pulley, and Jakka M. Vesala Cash, 'Paper and Electronic Payments: A Cross-Country Analysis' (1996) 28(4) Journal of Money, Credit and Banking 914.
[43] European Commission, *Towards an Integrated European Market for Card, Internet and Mobile Payments* (COM 941 2011) para 2.3.

internet, card networks and banks and non-bank e-payment service providers within e-payment systems.

It is important to state that there is generally no law which defines e-payments in Nigeria. Nevertheless, the definition provided by the Payment Systems Management Bill (which was never passed) provides an indication of the legal direction on e-payments in Nigeria. The bill defines payment systems as 'a system which enables payment to be effected between a payer and a beneficiary'.[44] It also defines 'electronic funds transfer' (EFT)[45] as;

> Any transfer of funds which is initiated by a person by way of instruction, authorisation or order to a *bank* to debit or credit *an account maintained with that bank* through electronic means and includes point of sale transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfers initiated by telephone, internet and card payment.[46]

It is important to note further that the definition (of ETF) under the proposed law appears to indicate that only *banks* will be engaged in ETF transfers and that there will always be some form of credit or debit account maintained by the customer at the bank. This assumption is erroneous and makes the definition deficient in a significant way. As will be argued later in this chapter, individuals can use e-payments without having any sort of account and providers of e-payment services are not generally limited to banks. The relevant arguments are integrated into the discussion on institutional arrangements below and are not considered further here.[47] Further analysis below considers the legal status of e-payments and the limitations if any on its use and enforceability.

2.3.2 Legal Status of E-payments

The major attributes of legal tender money are that it is accepted by virtue of legislative fiat and without the need to inquire into title except where it is counterfeit.[48] The primary question here is whether e-payments automatically function as money as a matter of social or industry practice or whether it is a legally recognised and binding form of payment in Nigeria.

---

[44] s 1 Payment Systems Management Bill 2009.
[45] EFT is used as a generic term synonymously with e-payment.
[46] s 1 Payment Systems Management Bill 2009 (emphasis added).
[47] See further notes below in 2.3.4.4 Payment Institutions – Institutional Framework for E-Payment Systems in Nigeria at p 37.
[48] Proctor, (n 35) 39-42.

Under the CBN POS Guidelines, all merchants are mandated to accept cards in payment for goods and services.[49] The regulation provides that 'Merchants shall accept cards as a method of payment for goods and services …A merchant shall under no circumstance ... discriminate against any member of the public who chooses to pay with a card or by other electronic means'.[50] As noted previously, it is legislation which compels the acceptance of money as an instrument of payment. To answer the question therefore, it is important to understand the current concept of legal tender in Nigeria.

The Central Bank of Nigeria (CBN) Act established the legal tender status of the Nigerian currency, the Naira. The Act provides;

> The unit of currency in Nigeria shall be the Naira... The Bank shall have the sole right of issuing currency notes and coins throughout Nigeria and neither the Federal Government nor any State Government, Local Government, other person or authority shall issue currency notes, bank notes or coins or any documents or tokens payable to bearer on demand being document or token which are likely to pass as legal tender.[51]

The Act further provides;

> The currency notes issued by the Bank shall be legal tender in Nigeria at their face value for the payment of any amount …[and] A person who refuses to accept the Naira as a means of payment is guilty of an offence and liable on conviction to a fine of N50, 000 or 6 months imprisonment.[52]

These provisions indicate that all payments are liable to be made in cash and there is a statutory obligation to accept cash in payment. As a general rule therefore, a creditor is not bound to accept payment otherwise than by legal tender currency.[53] By juxtaposing the foregoing provisions of the CBN Act and that of the POS guidelines, one can make a case for and against the legal status of e-payments relative to cash payments. On the one hand, one may argue that the guidelines cannot have the effect of compelling the acceptance of e-payments. This is because legal tender is strictly defined as bank notes and coins issued by the Central Bank of Nigeria. The clear terms of statute therefore exclude payment

---

[49] See items 4.5.2, 4.5.3 CBN POS Guidelines 2011.
[50] ibid items 4.5.2 & 6.
[51] ss 15 & 17 CBN Act.
[52] ibid ss 20(1), 20(5).
[53] ibid.

instruments issued by other private or public authority. By inference, payment instruments such as electronic money or pre-paid cards issued by private institutions cannot be money and there is no obligation to accept them in payment.

On the other hand, and in favour of enforcing the acceptance of e-payments, one can also infer a positive interpretation of the mandatory acceptance clause in the POS regulations. It can be argued for instance that while legislation may define legal tender, this does not preclude regulations from prescribing the acceptance of other forms of payments or payment instruments. As Hove rightly argues, the concept of 'legal tender' as it exists today - for traditional cash - can differ significantly from country to country.[54] Cohen also debunks the state theory of money.[55] He maintains that the modern concept of money is that money is whatever people come to believe will be accepted by others for whatever reason. He argues that consequently, state power is by no means the only source of trust in money.[56] As was also observed by the court in Reference *Re Alberta Statutes*,[57] money has a wider meaning than legal tender money. Accordingly, Proctor argues that with developments in technology and the amplification of means of payments, the meaning of money will correspondingly expand.[58]

The above observations are consistent with the view that money or currency does not constitute the only instrument of payment. Again however, even if one concedes that e-moneys are effective payment instruments, this cannot be construed to also mean that the law will enforce them or compel the acceptance of cash alternatives. It is therefore possible to interpret the provisions of Items 4.5.2 and 6 of the CBN POS guidelines cited above, to mean that a merchant can make a choice between both forms of payment and he is not obliged to accept one or the other. It is difficult to conclude whether or not this is the correct interpretation of the status of e-monies and e-payments in Nigeria. Legal and judicial authorities from other jurisdictions are also unhelpful in this regard as they present conflicting notions and opinions.

---

54 Leo Van Hove, 'Making Electronic Money Legal Tender: Pros and Cons' (Economics for the Future - Celebrating 100 years of Cambridge Economics, University of Cambridge September 17-19 2003) 5, <http://www.ibrarian.net/navon/paper/Making_electronic_money_legal_tender__pros___cons.pdf?paperid=1674497 dge> accessed 06/04/2015.

55 George Knapp, *The State Theory of Money* cited in Benjamin J. Cohen, 'Electronic Money: New Day or false Dawn?' (2001) 8(2) Review of International political Economy 197, 202.

56 ibid.

57 [1938] 100,116 cited in Proctor, (n 35) 13.

58 ibid 9.

It has been suggested for example that electronic moneys are neither money nor payment, and non-cash payments, although important from an economic point of view are of 'a different and minor legal quality'.[59] It has also been argued that it is the right to be paid money rather than money itself that is pushed around the payment systems.[60] Goode suggests that the intangibility of electronic payments leads to some confusion. As he observes, 'We also use terminology which confuses the payment message with the act of payment. Thus bankers refer to wire transfers and electronic funds transfers, conjuring up a picture of electronic currency, invisible and intangible, hurtling through the ether![61] Harry Leinonen expresses the view that, '...in a completely e-based system...Both money and payments have been transformed into a row of bits processed in a large network of numerous interconnected computers.'[62]

Judicial authorities have also not been unequivocal in their approach. In *Foskett v Mckeown* the court expressed the view that neither money nor property passes through the payment systems which are in fact "a series of debits and credits that are causally and transactionally linked."[63] The decision in *R v Preddy*,[64] appears to suggest that 'funds' in electronic fund transfer systems cannot be stolen. Although, legislation was passed to overrule the courts in some cases,[65] the foregoing observations suggest that the question of whether or not e-payment is money is not merely academic or tenuous. As the authorities indicate, technical interpretations may still inhibit the full acceptability of e-payments because they may be deemed mere payment processes or mechanisms which do not have the effect of crystallising into money.

2.3.3 Money as a Social Construct

Both legal and economic literature make useful proposals regarding the ways to navigate the trajectory, that is, whether e-payments have the same effect as money or otherwise. Geva's correct assessment is that the concepts of e-money and legal tender are not inherently

---

59 Gramlich, (n 37) 41.
60 Rhys Bollen, 'The Development and Legal Nature of Payment Facilities' (2005) 16 Journal of Banking and Finance Law and Practice 130.
61 Roy Goode, *Commercial Law* (3rd edn, Penguin Books 2004) 449.
62 Harry Leinonen, 'Payment Habits and Trends in the Changing e-landscape 2010+' (Helsinki Expository Studies A: 111 2003) <http://www.suomenpankki.fi/pdf/157714.pdf.> accessed 01/05/2014.
63 *Foskett v Mckeown* (2001) 1 AC 102, 128 [Millet LJ].
64 (1996) 3 All ER 481.
65 See eg Fraud Act 2006 which repealed s 15A Theft (Amendment Act) 1996 and overruled the House of Lords decision in *R v Preddy*.

incompatible since not all money is legal tender money.[66] For some legal scholars however, the solutions appear to be more direct. They canvass a strict adherence to the concept of legal tender money by creating a legal tender status for electronic moneys. Proctor argues for example that for money to function as a medium of exchange, a store of value or unit of account, it requires the authority of law or the state.[67] In other words, a state issued or state recognised legally enforceable electronic money system. Although rational, this position finds little support in the literature and will arguably be difficult to promote in the Nigerian context. First as discussed above, cash is legal tender which cannot be lawfully refused, and is in fact legally mandated to be accepted for all transactions. Therefore, a parallel regime of legal tender status for electronic money may create legal inconsistencies. Second, because of the nascent stage of development of e-payments, there is little doubt that given a choice, merchants will prefer the well-recognised and easily identifiable 'hard cash' to the more volatile electronic moneys or fund transfer systems.

Consequently, while conferring legal tender status on e-payments or e-moneys may admittedly address the conjectures surrounding the legal status and effect of e-payments, such an approach is unpersuasive and is unlikely to become generally accepted. One argument supporting this position stresses stakeholders' disposition to the continued existence of cash. It was argued that it is improbable that Central Banks will be willing to dispose of their powers to issue legal tender currency as this serves an economic as well as a social function. According to the Reserve Bank of New Zealand, 'Reserve Bank provision of currency under a statutory monopoly is seen as a useful public service and one which provides a basis on which other payment arrangements and contracts must ultimately rest.'[68] Regarding the position of users as stakeholders, it was also argued that the main incentive for cash is anonymity, and since 'anonymity will always be in demand', it (anonymity) will keep currency in being.[69] In essence, user demand will keep legal tender currency viable without more. As Goodhart and Krueger further argue, the one circumstance where one might expect information technology to bring an end to the use of national currency would be when an (authoritarian) government prescribes that all transactions must go through an

---

[66] Geva, (n 41) 13-20.
[67] Proctor (n 35) 9.
[68] Ledingham, (n 33).
[69] Charles Goodhart and Malte Krueger, 'The Impact of Technology on Cash Usage' (2001) London School of Economics Discussion Paper 374, 13 <http://eprints.lse.ac.uk/25048/1/dp374.pdf> accessed 07/04/2015.

electronic devise.[70] They concluded that indeed cash cannot be eliminated because they cannot be refused legally.

As a middle ground for the above arguments and as an alternative to making e-moneys legal tender, it has been proposed that the new forms of money be allowed to achieve acceptance through a process of self-recognition. The rationale for this position is that money is a social rather than a legal construct, therefore, by a process of evolution, electronic means of payment will achieve self-recognition independently of the concept of legal tender.[71] According to Weatherford, 'money is a system of thought, a way of organising social behaviour, and an integral part of modern culture, but money need not necessarily be an object'.[72] To support this position, one may consider a practical analogy. When we speak of payment, we think of parting with money. In the same way when we make e-payments, we think we have parted with money and not information or data or whatever designation may be assigned to e-moneys and e-payments. Also, if we are dispossessed of cash or currency, we think of it as theft or fraud, if our payment card is stolen, we also do not think we have lost information, we think of it as a potential loss of money whether in an account or on the card. This demonstrates that 'money' takes its meaning from context and the term resides in function rather than form.[73]

However, as Goodhart and Krueger argue, social recognition of e-payments will not develop in a vacuum. The way to achieve the needed recognition is to strive for the establishment of an effective legal framework which boosts acceptability of e-payments by creating a positive response linked to the government.[74] Such a framework has the potential to establish viable competition between e-payments and its more entrenched competitor, cash,[75] and to change perceptions of e-payments whether or not they are accorded legal tender status.[76] According to Ledingham, the specific framework for the success of e-payments are rules relating to security of electronic transactions particularly those which deal with risks and liabilities. As he argues;

---

[70] ibid.
[71] ibid.
[72] Jack Weatherford, 'Dump Bronze Age Bucks for Electronic Money' (USA Today Apr. 1993: 13A) cited in Barbara A. Good, 'Will Electronic Money Be Adopted in the United States?' Federal Reserve Bank of Cleveland Working Paper 9820, 6.
[73] See eg *Suffel v Bank of England* (1882) 9 QBD; see also *Reference Re Alberta Statutes* [1938] 100,116 cited in Proctor (n 35) 13.
[74] Goodhart and Krueger (n 69).
[75] See Van Hove (n 54).
[76] See Benjamin Geva, 'Legal Aspects Relating to Payment by E-Money: Review of Retail Payments System Fundamentals' (2001) Int'l Fin & Econ L 5 Y B 255.

> Any arrangements for making monetary payments require satisfactory legal underpinnings. It is important that all of the parties to a payment - the payer, the recipient, and any other parties such as banks or clearing systems who may be involved as intermediaries - clearly understand their rights and obligations, and any risks they may face. The rules need to specify clearly who carries risks at the various stages that a transaction may pass through, and what happens when things go wrong.[77]

In effect, the formulation of rules which establish liability structure, particularly in cases of fraud and theft are essential to the functioning and acceptability of the systems. The sections below examine the classifications of e-payment systems and institutional arrangements for e-payments in Nigeria. It is argued that the CBN regulations and other banking and financial regulations are inadequate to regulate new e-payment service providers and the threats they pose to the payment system.

2.3.4 Classifications of E-payment Systems

E-payment systems are complex because they cover a wide range of payment institutions, payment mechanisms and payment instruments, and are driven by technological changes and modifications. Classifications of the systems have therefore been based largely on the subject perspective of writers, [78] the jurisdictions which are the subject of inquiry or the literature consulted.[79] However, according to the European Central Bank (ECB), '...it is becoming increasingly difficult to categorise e-payment services, since formerly specific functions and distribution channels are blurring and merging to create hybrid products, multi-channelling and new role-sharing models.'[80]

Based on the complexity indicated above, an incursion into the extensive and diverse body of literature on the classifications and categorisation of e-payment systems is unnecessary because it is impossible to replicate existing classifications to a greater or lesser extent. It is therefore more useful, for the purpose of highlighting the legal issues involved, to classify e-

---

[77] Ledingham (n 33) Para 32.
[78] This may be legal, technical or scientific or economic perspective.
[79] See eg Andrew G Haldane, Stephen Millard and Victoria Saport (eds) *The Future of payment Systems* (Routledge International Studies in Money and Banking 2008); see also Dennis Abrazhevich, *Electronic Payment Systems: A User-Centered Perspective and Interaction Design* (Eindhoven 2004).
[80] European Central Bank (ECB), 'E-payment Without Frontiers' (Issues Paper for ECB Conference 10 Nov 2004) 4 <https://www.ecb.europa.eu/events/pdf/conferences/epayments2004/epaymentsconference-issues2004en.pdf > 12/06/2015.

payment systems based on their broad and generic characteristics in Nigeria. These are one; the purposes served by the systems, whether retail or wholesale payments. Two, the channel of payment, whether they are offline or online e-payment systems. Three, the instrument of payment, that is, whether they are account based or electronic money system. Four, the institutions involved in providing the services, whether they are banks, or non-bank financial institutions or non-financial institutions.

2.3.4.1 Purpose served by Payment -Wholesale and Retail Systems

Wholesale systems are used for large electronic transactions and often involve interbank clearing and settlement systems. They use the Inter-Bank Settlement System Electronic Fund Transfer (NEFT) similar to the Federal wire clearing House Interbank System (CHIPS) in the US, and the Clearing House Automated Payment System (CHAPS) in the UK. Retail e-payments are devised for low-value consumer payments such as payment for goods and services, bill payments, peer to peer payments and payments at points of sale. Relative to wholesale payments, retail payments are higher in volume but lower in value. They are implemented using different payment instruments and channels particularly payment cards, Automated Teller machines (ATMs) and points of sale networks and terminals which are discussed further below.

2.3.4.2 Payment Channels - Online and Offline Systems

Electronic payments are further distinguished as online or offline systems. Online systems require real time authentication for payment to be completed.[81] Offline payments include payments by cheques, cash or payment on delivery. It is significant to mention that the adoption of payment channels such as Automated Teller machines (ATMs), points of sale and mobile phones have increased access to online payment systems in Nigeria. Conversely, the channels have implications for security of users and consumers of e-payment services. For example, theft and fraud in financial transactions increased at an unprecedented scale since the introduction of ATMs in Nigeria. Between 2010 and 2012, ATM fraud was the most pervasive form of fraud on electronic payment channels and the leading consumer complaint to the Central Bank of Nigeria.[82] Similar security challenges are expected as points of sale proliferate and become more widely used in Nigeria. A point of sale (POS) is an electronic devise which enables participating merchants to process and accept payment cards as a means of payment for goods and services. Due largely to low deployment of the

---

[81] See further notes in (a) Authenticating Technologies p 76.

[82] See Nigeria Deposit Insurance Corporation, 'Annual Report and Statement of Accounts 2010, 2011 and 2012' <http://ndic.org.ng/publications.html> accessed 12/09/2013.

terminals and reluctance of merchants to use them, proximate POS, such as merchant terminals, are yet to achieve the expected levels of acceptance in Nigeria. However, mobile terminals such as mobile devices and virtual terminals such as the internet are increasingly used for banking and payments.

Mobile devices constitute points of sale when used to transfer funds or to pay for goods and services. Mobile phones in particular are used to access bank accounts, transfer funds, pay bills and make peer to peer payment on the internet. Mobile phones installed with near field communication (NFC) technology could also be used to make payments by interacting with POS terminals. Mobile payments are relatively new innovations but have been widely accepted in Nigeria. The increasing proliferation of mobile phones and the ability to dispense with bank accounts are the major factors driving the adoption of mobile payments. For example, the number of mobile phone subscription increased from about 1.5million in 2002 to almost 160million in 2013. Nigeria has over 180 million mobile phone subscribers as at February 2015. [83]

A number of user and security challenges are associated with mobile payments. User challenges include constraints imposed by lack of technical knowledge and the complication of mobile applications. Regarding security, mobile terminals presents challenges similar to other electronic devices such as computers. For example, mobile phones are susceptible to security breaches such as hacking which may render users liable for unauthorised or fraudulent transactions made through their phones. Also, payment applications developed for use on mobile devices are not currently subject to the Payment Card Industry Payment Applications Data Security Standards (PCIDSS).[84] More crucially, as argued later in this chapter, ambiguity surrounds the regulatory framework for mobile payment providers relative to banks and other financial service providers in Nigeria.

[83]See NCC, Subscriber Statistics <http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73>, accessed 24/05/2015.
[84] See PCI Security Standards Council, Payment Card Industry (PCI) PA-DSS Program Guide, v3.0 16-18 <https://www.pcisecuritystandards.org/documents/PA-DSS_Program_Guide_v3.pdf> accessed 03/02/2015.

2.3.4.3 Payment Instruments –Account Based and Electronic Money Systems

The proposed law on Payment Systems Management in Nigeria defines a payment instrument as 'an instrument, authority or a process enabling a payer to issue a payment instruction.'[85] Payment instruments can be account based or stored value systems.

Account based systems operate on pre-existing debit and credit system. They are described as notational systems where money is represented by records in bank accounts and transferred electronically as information over computer networks.[86] Account based systems may use debit and credit cards, or prepaid or stored value cards as well as smart cards. Debit cards are linked to and charge purchases of goods and service to the customer's account. They are the most commonly used payments cards in Nigeria and many proprietary ATM cards issued by banks also function as debit cards. Debit cards in Nigeria are also issued in conjunction with International card schemes particularly VISA and MasterCard. Whereas debit cards charge the holder's deposit with the issuing bank, credit cards represent a credit extended to the holder by the issuer of the card which allows a customer to purchase goods and services against a pre-set limit. Credit cards are not common in Nigeria. The most important factor contributing to this is lack of infrastructure for credit checks such as identification and address verification processes.[87]

Stored Value and Prepaid card are often used as generic terms for e-payment systems operated without a link to designated bank accounts. Precisely because they dispense with deposit accounts, prepaid and stored value cards are expected to gain popularity in Nigeria. For the unbanked population, which is established to be in the majority, the cards offer alternatives to conventional deposit accounts.[88] However, while prepaid and stored value cards are used interchangeably within the card industry, there is a clear distinction to be made between the two systems. Prepaid cards are issued to persons who deposit funds into an account of the issuer. The issuer collects personal information such as names, addresses, phone numbers and signatures during the fund deposit process. Stored value systems do not typically involve the deposit of funds or collection of personal information as value is stored

---

[85] s 1 Payment Systems Management Bill 2009.
[86] Clifford Neuman and Gennardy Medinvsky, 'Internet Payment Services' in Lee W McKnight and Joseph P. Bailey (eds) *Internet Economies (*Massachusetts Institute of Technology 1997*).*
[87] See eg Presidential Implementation Committee on the National Identity Management System, Consumer Credit System and National Outsourcing Initiative, 'National Policy and Institutional Framework for an Identity Management system for Nigeria' <https://www.nimc.gov.ng/sites/default/files/nimc_policy.pdf> accessed 06/04/2015.
[88] See notes on Promoting Financial Inclusion below.

directly on the cards. Therefore, although, the two systems have the prepaid element as a common denominator, prepaid systems use the physical card as a token to access value recorded remotely and linked to the card, and is largely analogous to account based systems. Stored value systems actually store and access value from the physical card's chip and are similar to electronic monies discussed below. [89]

The above distinctions are not implied in the regulatory guidelines in Nigeria. For example the CBN guidelines provide that both prepaid and stored value cards may be issued by banks and non-banking organisations. Under the guidelines, deposit-taking banks or financial institutions licenced by the CBN with clearing capacity may issue stored value/prepaid cards. Other deposit-taking institutions without clearing capacity may also issue the cards acting in conjunction with institutions having clearing capacity.[90] Mobile and telecommunications operators may also operate money transfer schemes with stored/value prepaid cards subject to obtaining the requisite approval of the CBN.[91] Although the Guideline recognises that stored value cards may be issued anonymously, it nevertheless requires that issuers of both stored value and prepaid cards fulfil minimum Know Your Customer (KYC) requirements.[92] That is, issuers must collect the names, addresses and telephone numbers of prospective users. As discussed below and more comprehensively later in the thesis, this process of collection of personal information by banks and non-banks, ostensibly for the issue of prepaid and stored value cards, raises fundamental questions about the security and protection of consumer information.

Generally, smart cards are multi-application cards embedded with micro-processing chips. They can be used for a number of purposes including e-payments. Smart cards have been classified based on whether they are single or multi-purpose cards, or closed or limited purpose cards, or according to whether they are contact or contactless cards or hybrid or proximity cards.[93] Multi-purpose smart cards are poised to play a vital role in the future of e-payments in Nigeria. For example, government has commenced the implementation of a multi-purpose national identity card scheme which would operate through the smart card

---

[89] See generally Wolfsberg Group 2011, 'Guidance on Prepaid and Stored Value Cards' <http://www.wolfsbergprinciples.com/pdf/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf> accessed 18/07/2011.
[90] Item 3.1 CBN prepaid/Stored Value Card Guidelines 2012.
[91] ibid item 3.9.
[92] ibid item 4.1 & 5.1.
[93] Phoebus Athanassiou and Natalia Mas Guix, *Electronic Money Institutions: Current Trends, Regulatory Issues and Future Prospects European* (ECB 2008) 7.

technology. The card will store fingerprints and biometrics information of the user. It will also have payment functionalities including serving as a bank card.[94]

As noted earlier, payment instruments can also be electronic money systems. Although, account based systems (discussed above) involve the use of some form of "electronic money", 'real electronic money' refers to token or stored value systems. It is rightly defined as '...electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument'. [95] Therefore, electronic currency is stored value or token systems similar to conventional cash. They are variously referred to as electronic cash, digital cash or electronic money.

Corresponding to this definition, electronic money in Nigeria is stated to mean monetary value stored electronically in a centrally held electronic devise.[96] To qualify as e-money, such stored value must have been issued on receipt of funds, accepted as a means of payment otherwise than by the issuer, be transferable, and have defined cash out capabilities.[97] The distinguishing qualities of e-money are its ability to mimic the anonymity of cash, suitability for micro-payments and lack of credibility requirements for users. In spite of its qualities and similar to developments in other countries, innovations to develop electronic currencies in Nigeria have been largely unsuccessful.[98]

For the specific purpose of the analysis here, it is important to mention that e-moneys can be issued by banks and non-banks. [99] When operated on mobile platforms, mobile money systems in Nigeria can be card account based, bank account based or stored value (e-money) based.[100] Card account based systems links payment cards to a mobile phone for the purpose of initiating and concluding payment transactions. Bank account based systems link payment instructions to the customer's bank account, whether current, savings or domiciliary accounts. In stored value account based systems, mobile moneys are driven by system based accounts such as pre-paid cards or reloadable value accounts.[101] Further

---

[94] See further notes in 5.1.1 NIMC's Electronic National Identity Card at p 137.
[95] European Central Bank, *Report on Electronic Money* (ECB 1998) 7.
[96] See Item 5.1 CBN Mobile Payments Regulations 2009.
[97] ibid.
[98] E-cash, Mondex, Pay Word, MicroMint and NetCash are examples of failed electronic money initiatives. Globally, Bitcoin is the most successful electronic currency system.
[99]See generally items 2.2.1-2.2.3 CBN Mobile Payments Regulations 2009.
[100]ibid item 2.2.
[101] ibid items 2.2.1-2.2.3.

analysis below demonstrates that this interconnection and interrelationship between mobile systems and financial services raise issues for law and regulation.

2.3.4.4 Payment Institutions – Institutional Framework for E-Payment Systems in Nigeria

Banks are still the dominant e-payment services providers in Nigeria, however, non-bank service providers are becoming increasing relevant. As noted above, non-bank service providers can issue stored value and prepaid cards. Mobile payment services can be also be operated solely by non-bank organisations approved by the CBN.[102] According to the Bank of International Settlement, declining hardware and software costs as well as greater expertise in developing related payment applications has increased the participation of non-traditional financial institutions and even non-financial institutions in payment services in some countries.[103] In Nigeria, these institutions act as payment intermediaries, they process payment transactions and may be collectors and processors of payment information. This development has certain implications for existing institutional arrangements in the payment industry.

To illustrate this, it is important to mention that three main sectors generally converge around e-payments. These are the banking industry, telecommunications sector and web services. As noted previously, the Central Bank of Nigeria (CBN) is the primary regulator of the Nigerian financial industry and to regulate e-payments, the CBN relies largely on the provisions of banking legislation, [104] and a patchwork of ad hoc regulations and guidelines.[105] While the various guidelines empower the CBN to licence payment services providers in Nigeria, under the banking laws, the CBN has no express powers to regulate nonbank or non-financial institutions. This apparent contradiction can be explained from two perspectives. It is possible to argue on the one hand that by virtue of its powers to regulate payment systems generally, all payment activities are subject to regulation by the CBN.[106] This is particularly so in view of the provision of section 2(d) of the CBN Act which states that the promotion of a sound financial system is one of the objectives of the Central Bank.[107] Under section 47(2), the Act also provides that '... in furtherance of the

---

[102] ibid items 2.3.1.1, 3.2.2.1, 3.2.2.3.
[103] Committee on Payment and Settlement Systems, *Retail Payments in Selected Countries: A Comparative Study* (Bank of International Settlement 1999) 17.
[104] These are Central Bank of Nigeria Act Cap C4 LFN 2004 (hereinafter CBN Act) and the Banks and Other Financial Institutions Act Cap B3 LFN 2004 (hereinafter BOFIA).
[105] See notes in 2.2.1 Development of Banking and Payment Systems in Nigeria p21 at 23.
[106] See s 47 CBN Act.
[107] ibid s 2(d).

provisions of section 2(d) of this Act, the Bank shall continue to promote and facilitate the development of efficient and effective systems for the settlement of transactions (including the development of electronic payment systems)'.[108]

On the other hand, it may be argued that since some service providers are neither banks nor other financial institutions, they cannot be subject to CBN regulation. Under the laws, the CBN is only empowered to regulate banks, banking business and other financial institutions.[109] A bank is defined under the CBN Act as 'a bank' licensed by the CBN.[110] Banking business also means;

> ...the business of receiving deposits on current account, savings account or other similar account, paying or collecting cheque drawn by or paid in by customers; provision of finance or such other business as the Governor may, by order published in the Gazette, designate a banking business.[111]

In contrast to the above definition, many e-payment service providers are usually non-deposit taking and may not maintain any form of customer account. In the strict sense therefore, payment services may be merely ancillary to their core activity. This means in effect that the CBN can neither license a non-bank or non-financial institution payment service provider, nor enforce financial regulations on the relevant service provider. The point highlighted here can be illustrated by e-money schemes in Nigeria. In e-money schemes, issuers may adopt one of the three mobile money models. They can operate the bank-focused model, where a bank delivers banking services to existing and prospective customers using the mobile phone as a delivery channel. This model can only be deployed by licensed deposit-taking financial institutions including deposit money banks, microfinance banks and discount houses.[112] Issuers of e-moneys may also adopt the bank-led model where banks, or a consortium of banks, partnering with other organizations, jointly seek to deliver banking services leveraging on the mobile banking system.[113] The third model which is the non-bank led model is of particular interest. The model allows corporate organisations that have been duly approved by the CBN to deliver mobile payments services to consumers. It can only be operated by organisations other than

---

[108] ibid s 47(2).
[109] See ss 1, 2 & 59 BOFIA.
[110] See s 60 CBN Act.
[111] s 66 BOFIA.
[112] See item 2.1 CBN Mobile Payment Regulations 2009.
[113] ibid item 2.1.2.

licensed deposit money banks and telecommunication companies.[114] Therefore, in the strict sense, telecom companies are excluded from participating as lead providers in e-money schemes in Nigeria.[115] Nevertheless, they may operate as value and mobile money service providers in conjunction with banks while playing the major role of providing network infrastructure for the use of the scheme. [116] The question then is to which regulatory authority are such mobile network providers subject particularly when it comes to protecting users' (personal) information?

To further highlight how law, policy and regulation may conflict on the critical issue of regulation, the provisions of current CBN regulations and that of the Payment Systems Management Bill noted earlier in this chapter, may be examined. The CBN regulations recognise non-bank participants in the payment industry. These participants including merchants, merchant acquirers, switching companies, and POS terminal owners and payment service terminal aggregators and providers are referred to as 'stakeholders' in the Nigerian payment industry. [117] However, as noted in the analysis of the definition of e-payment systems above, the law then proposed to regulate payment services, the Payment Systems Management Bill, defines electronic transfer of funds (ETFs) without recognition of the roles of these industry stakeholders.[118] The Bill defines ETFs rather restrictively as, '… any transfer of funds which is initiated by a person by way of instruction, authorisation or order to a *bank* to debit or credit *an account maintained with that bank* through electronic means...'.[119] This definition suggests that only banks are involved in EFTs and the user of a payment service must have some sort of account with the bank. This is in direct contrast to the realities of the e-payment industry. As discussed earlier, modern e-payment instruments do not necessarily require that the holder have an account held at a bank. All that is required is a form of account which can be debited or credited. This may be a card account or a system account.

The provisions of the Payment Services Regulations (PSR) (UK) further clarify the point here. The PSR defines payment services to include the issuing of payment instruments or acquiring payment transactions, offering mobile or fixed phone payments and payments

---

[114] ibid item 2.1.3.
[115] ibid.
[116] ibid item 2.1.
[117] See items 2 & 3 CBN POS Guidelines 2011.
[118] See notes in 2.3.1. What is E-Payment (Systems)? p 23 at 25.
[119] s 1Payment Systems Management Bill 2009 (emphasis added).

from other digital devices as well as money remittance services.[120] The main advantage here is that the law clearly defines categories of payment service providers rather than a general and ambiguous categorisation of "industry stakeholders" adopted in the CBN guidelines. Furthermore, the PSR did not delimit payment services and fund transfers to banks and other financial institutions. It recognises and includes remittances made using IT infrastructures and delineates such transfers as payment services irrespective of the involvement of banks. From this perspective, one may argue that even if it intends to exercise regulatory powers over non-banks, the provisions in its proposed payment service bill amounts to the CBN literally "shooting itself in the foot". The provision would be restrictive in the sense that it fails to take cognisance of other activities which may constitute transfer of funds, or of other organisations which may offer payment services.

According to the CBN itself, telecom providers were excluded from leading mobile money services specifically to prevent a regulatory collision with the Nigerian Communications Commission which regulates telecommunication.[121] However, this explanation only furthers the argument that a lacuna will then exist in regulation. In essence, if the CBN cannot regulate payment services offered by industry subject to other regulators, it means such services would either be largely unregulated or left to regulators without expertise to monitor payment services. In chapter five, the data protection implications of the national electronic identity card, the Subscriber Identity Module (SIM) registration and the biometric verification code are analysed to highlight the problems in the context of regulating the processing of personal information.[122]

For the purposes of concluding the arguments here, it is relevant to note, as suggested by some commentaries, that e-payments and e-money systems erode the powers of Central Banks. As far back as 1996, Hughes had argued that new e-payment mechanisms challenge traditional banking activities because the new mechanisms not only operate outside the scope of national laws that apply to banking transactions, but also impact on laws that promote safety and soundness.[123] Kobrin had also argued, quite emphatically, that new payment systems will eventually displace the relevance and powers of central banks and

---

[120] Payment Services Regulations 2009 SI 2009/209, sch 1 pt 1 para 1(a)-(g).
[121] See Mobile Banking: Why we did not Licence MTN, Others, CBN <http://mobilemoneyafrica.com/mobile-banking-why-we-did-not-licence-mtn-others-cbn/ > accessed 12/06/2012.
[122] See further notes in 5.1 Challenges of Data Protection in E-payment Systems in Nigeria p 135.
[123] Sarah Jane Hughes, 'A Call for International Legal Standards for Emerging Retail Electronic payment systems' (1996) 15 Ann Rev Banking L 198.

render them dispensable in the regulatory scheme for new payment systems.[124] Although, this assessment is exaggerated, it is mostly correct. For example, while it can be argued that central banks will continue to be relevant because cash will remain in demand, it is also reasonable to argue that central banks, such as the CBN, are incapable of regulating the broad scope of services and providers involved in e-payment systems. A contrary approach is likely to deepen the regulatory lacuna which can be exploited either by the institution/providers themselves or by criminal/outsiders. The correct conclusion must be that participation of nonbanks institutions poses particular risks to e-payment because they provide alternative points of entry into payment systems for criminals.[125] In the context of payment security and privacy therefore, the question of how or the extent to which e-payment service providers should be regulated is important. The concluding section of this chapter highlights the significance of e-payment to growth and development in Nigeria.

2.4 E-payment Systems and Development in Nigeria

The main advantages of electronic payment systems are its speed, efficiency and elimination of congestion and handling charges associated with the clearing of paper cheques. Its pragmatism in avoiding the use of cash and the risks associated with cash is another of its fundamental advantages. E-payments also facilitate business and payment processes, and have become a key mover of the information society because they are essential infrastructure for electronic commerce.

The adoption of e-payment systems in Nigeria is centred on two main considerations. These are one, the need to achieve control and regulation of monetary policies, and two, the need to promote the digital economy in line with global trends.[126] The following sections examine how these translate to specific economic and developmental advantages.

2.4.1 Consumer Convenience

It is trite that relative to e-payments, cash is cumbersome. It is also trite that in contrast to the anonymity of cash, e-payments leave audit trails which forestall or aid the resolution of disputed payment claims. Furthermore, because of its capacity to effect instant payments, e-payments engender confidence in the non-reversibility of payments and thereby guarantee

---

[124] Stephen J. Kobrin, 'Electronic Cash and the End of National Markets' <http://www.jstor.org/stable/10.2307/1149333> assessed 11/02/2012.
[125] See eg Weiner et al, 'Nonbanks and Risk in Retail Payments' (2008) Federal Reserve Bank of Kansas City Working paper 07-02.
[126] See Central Bank of Nigeria, 'Payment Systems' <http://www.cenbank.org/Paymentsystem/> accessed 12/05/2012.

the finality of transactions. Finally, because consumers are likely to handle less cash, the use of e-payment systems has the potential to reduce the incidence of robbery and theft in Nigeria. As the CBN observed, the adoption of e-payments by consumers is expected to lead to increased convenience, more service options, reduced risk of cash-related crimes, and cheaper access to banking services. The services are also expected to lead to increased access to credit and financial inclusion. In terms of convenience therefore, e-payments are expected to deliver payment services that are relatively safe, efficient and fast for the Nigerian consumer.

2.4.2 Reduction in the Cost of Cash

From economic and fiscal perspectives, cash was adjudged an inefficient form of payment. According to the CBN, the cost of cash had continued to rise and was projected to hit an all-time high (about 192 billion Naira (approximately 1.4 billion USD) in 2012.[127] A major objective of various policy implementations and development of technical infrastructure in the area of e-payments is therefore to reduce the cost of cash handling. As noted in a research conducted by Humphrey et al, the social cost of cash relative to that of e-payments is one of the major justifications for adopting e-payments. Commenting on the cost advantages of a switch to e-payments in some European economies, the authors observed:

> If a country is able to shift from an all paper- based to an electronic-based payment system, annual savings of perhaps 1% of GDP can be realised. This is because electronic payments, depending on application (point of sale, bill payment, or even employee disbursement) are from one half to two-thirds lower than their alternative paper-based non cash instrument.[128]

2.4.3 Promoting Financial Inclusion

The development of e-payment systems is both a social and a political process and evidence points to the usefulness of e-payment systems as a tool for developing new banking culture, achieving financial inclusion and enhancing governance.[129] The Financial Action Task

---

[127] See Central Bank of Nigeria Press Release on Cash Collection Policy <http://www.cenbank.org/Out/2011/pressrelease/gvd/PRESS_STATEMENT_ON_THE_NEW_CBN_CASH_COLLECTION_POLICY.pdf > accessed 12/06/2012.

[128] David Humphrey et al, 'Cost Savings from Electronic Payments and ATMs in Europe' (2003) Federal Reserve Bank of Philadelphia Working Paper 03-16, 2.

[129] Eg Kenyan M-Pesa reportedly reduced the population of financially excluded from 60% in 2006 to 25% in 2013, see Katrina Manson, 'Mobile Phones are Route to Financial Inclusion for Kenyans' *Financial Times* (London, 25 Novemeber 2013)<http://www.ft.com/cms/s/0/6cd723d8-5049-11e3-9f0d-00144feabdc0.html#axzz3VJ1Rnu7T> accessed 24/03//2015.

Force (FATF) defines financial inclusion as access to financial services at an affordable cost in a fair and transparent manner. It involves taking into account the under-served, undocumented and disadvantaged and vulnerable groups in the provision, availability, affordability and convenience of payment services.[130] Together with financial literacy, financial inclusion has been identified as an important index for economic development and eradication of poverty.[131]

For Nigeria, these observations translate into one major advantage, the use of e-payment to facilitate the integration of the unbanked population into the financial sector. Research indicates that out of 80 million adult Nigerians, 64.1 percent which represents 56.3 million adults do not have a bank account.[132] The main reasons for this include the historical attachment to cash, imbalances in rural/urban development resulting in the concentration of banks and other financial institutions in cities and big towns, illiteracy, and until very recently, a lack of political will on the part of the government to initiate necessary reforms in the payment systems.

Corresponding to the attainment of financial inclusion is the ability of regulatory authorities to better perform effective oversight functions. In other words, financial inclusion enables regulators to monitor the funds in circulation and foreclose on the informal economy. Other far reaching implications of financial inclusion include increase in subscriber base for e-services, support for privatisation and liberalisation and the promotion of foreign investments as well as the development and sustenance of e-governance initiatives.[133] Arguably therefore, with the potentials of ICT integrated payment systems, the Nigerian financial industry is a prospective foreign investment yield.

2.4.4 Developing E-commerce

According to the OECD, developing economies can leverage ICT to leapfrog the digital gap. One of the ways in which they can achieve this is by participation in e-commerce. Also, according to the OECD, e-commerce will ultimately form one of the indices for adjudging

---

[130] See World Bank/Financial Action Task Force (FATF) 'Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion' (OECD/FATF 2013) <http://www.fatfgafi.org/media/fatf/documents/reports/aml_cft_measures_and_financial_inclusion_2013.pdf> accessed 07/03/2015.

[131] See eg Micheal Chibba, 'Financial Inclusion, Poverty Eradication and the Millennium Development Goals' (2009) 21(2) European Journal of Development Research 21.

[132] See Central Bank of Nigeria Microfinance Policy Framework for Nigeria Revised April 2011<http://www.cenbank.org/Out/2011/publications/dfd/Reviewed%20Microfinance%20Policy%20July%2012%202011.pdf> accessed 21/04/2012.

[133] See eg Gramlich L, (n 37).

economic growth.[134] E-commerce generally refers to commercial transactions occurring over electronic networks, particularly the internet. It includes the sale or purchase of goods or services conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. E-commerce transactions can be between enterprises, households, individuals, governments, and other public or private organisations.[135] Depending on the parties to the transaction, e-commerce business models may include business to business (B2B), business to consumer (B2C), and consumer to consumer models. Others such as government to citizens (G2C), government to business (G2B) and government to government (G2G) involve transactions with or between governments.[136]

As far back as 2001, the UNCTAD identified the potential of B2B e-commerce to reduce the marginalisation of producers from developing economies by enabling them to compete in the global market.[137] However, corresponding to increasing internet access, B2C e-commerce is growing and also poised to meet similar developmental needs. E-commerce started effectively in Nigeria in 2010 and has developed in terms of number of participating e-retailers, merchants and consumers. E-retailers such as Jumia.com and Konga.com operate Amazon type platforms and claim to be filling combined orders of over 1000 a day only few months after their launch.[138] E-commerce in Nigeria has also attracted significant foreign investment. Reports from the financial industry indicate an increase in online payments from $314million in 2010 to $488million in 2012. A projected rise to $630million was made for 2013.[139]

The above developments imply that for an evolving digital economy such as Nigeria, secure and efficient e-payment mechanisms would further drive e-commerce in particular and economic growth in general. At the level of the financial industry, e-payment solutions that serve e-commerce spur innovation and promote competitiveness. Already

---

[134] OECD, *Guidelines to Measuring the Information Society* (OECD Publishing 2011).
[135] ibid 72.
[136] See OECD, 'Glossary of Statistical Terms' <http://stats.oecd.org/glossary/detail.asp?ID=4722> accessed 16/04/2012.
[137] See United Nations Conference on Trade and Development (ŬNCTAD), 'E-Commerce and Development Report 2001' <http://unctad.org/en/docs/ecdr2001_en.pdf> accessed 29/11/2014.
[138]See Xan Rice, 'Internet Sales Flourish in Nigeria' *Financial Times* (London, 13 May 2013)<http://www.ft.com/cms/s/0/3f455b7e-b1bb-11e2-9315-00144feabdc0.html#axzz3KV2wH7cP> accessed 29/11/2014
[139] See Eromosele Abiodun, 'E-commerce Attracts N8.25bn Foreign Investments' *This Day Newspapers* (Lagos, 27 March 2014) <http://www.thisdaylive.com/articles/e-commerce-attracts-n8-25bn-foreign-investments/174641/> accessed 29/11/2014.

in Nigeria, consumers have a wide array of choice between stored value and pre-paid cards. At governmental levels, e-commerce makes governments and their agencies proactive and creative. New technologies demand new laws and new entities need to be licensed and regulated. In appropriate circumstances, government could levy fees, charges, penalties and taxes, and thereby potentially expand its revenue base. For businesses, a major advantage of e-commerce is the growth of small and medium sized businesses through expansion of potential geographical markets. The accompanying reduction in the cost of access saves the overhead costs of doing business particularly the cost of store rental and personnel for small businesses. Individuals could also be gainfully (self) employed as e-retailers making e-commerce a major entrepreneurship and micro-enterprise driver. It is therefore not difficult to understand how increased global access aided by payment modernisation can lead to poverty eradication, job creation, and perhaps an end to monopolies of traditional banking and payment services.

It is notable that in spite of its advantages, a major setback for e-commerce in Nigeria is the slow uptake of online payment systems. While payment for goods and services bought online could be made offline, this is generally considered less efficient than online payments. In Nigeria however, most consumers still prefer to pay cash-on-delivery and e-retailers encourage this simply to speed up the growth of their businesses.[140]Acceptance of new payment systems is also marginal because providers and/or their products are new and trust issues exist. If unaddressed, these acceptance challenges may manifest as the "chicken and egg" effect. A payment system exhibits "chicken and egg" or 'network effects' when no one wants to belong to the payment network or use a payment instrument or process unless lots of other parties already use the system. Ultimately because everyone waits for others to use the system, it never gets used.[141] Arguably therefore, breaking the deadlock and overcoming the chicken-and-egg effect entails addressing factors, such as insecurity and trust which precipitate adverse choices. As will be argued later in the thesis, this would involve laws and regulations which strengthen security and promote trust online.

---

[140] See Ben Uzor, 'E-retailers Switch Tactics as Mistrust of Online Shopping Hamper Growth' *Business Day* (Lagos, 21 March 2014) <http://businessdayonline.com/2014/03/e-retailers-switch-tactics-as-mistrust-of-online-shopping-hamper-growth/> accessed 30/11/2014.

[141] Michael L. Katz, 'Increasing Connectedness and Consumer Payments: An Overview' (Proceedings of International Payment Policy Conference Kansas City March 29-30 2012), 23.

2.4.5 Controlling Crime

Perhaps one of the most controversial justifications for promoting e-payment systems is its ability to serve as an instrument of crime control. According to the CBN, e-payments can curb the risks of violent crimes such as theft and bank robbery.[142] In other words, since criminal associations prefer cash payments on account of its associated anonymity, e-payments can be useful in mitigating the prevalence of economic and organised crimes such as money laundering, kidnapping, drug dealing and terrorist financing. E-payments perform these functions by creating audit trails and eliminating the anonymity associated with cash transactions.

While the justifications underlying the crime control functions of e-payment systems are logical, the argument has a flip side. Firstly, anonymity, which is sought to be eliminated by e-payment systems, is as much a concern of individuals and legitimate businesses as it is of criminals. It is therefore not necessarily logical to associate desire for payment anonymity with criminal inclinations. Secondly, available evidence suggests that e-payments aggravate rather than reduce crimes, particularly theft and fraud. The Financial Action Task Force (FATF) reported in 2010 that pre-paid cards and mobile and internet payment systems are vulnerable to abuse and are being used for money laundering and terrorist financing. The biggest of the reported cases involved USD 5.3million.[143] Also, in 2010, ATM fraud accounted for more than 50% of the total loss to fraud and forgeries in the Nigerian financial sector.[144] Therefore, as the internet has greater propensity to facilitate criminal behaviour, it is rational to expect that e-payment systems would be further exploited by criminals. This calls for an examination of the various modalities which are currently employed or which may be used for crime prevention, detection and reaction in e-payment systems.

Conclusion

This chapter serves the purpose of introducing the Nigeria legal system as a foundation and reference point for later analysis in the thesis. It examined the constitutional, legislative and judicial arrangements within the Nigerian legal system and highlighted the links between

---

[142] Central Bank of Nigeria, 'Further Clarifications on the Cashless Lagos Project' <http://www.cenbank.org/cashless/> accessed 21/05/2012.
[143] Financial Action Task Force (FATF), 'Money Laundering Using New Payment Methods'(2010)<http://www.fatfgafi.org/media/fatf/documents/reports/ml%20using%20new%20payment%20methods.pdf.> accessed 08/12/2013.
[144] Nigeria Deposit Insurance Corporation (NDIC), 'Annual Report and Statement of Account 2010'<http://ndic.org.ng/files/NDIC%20Annual%20Report%202010.html> assessed 10/09/2012.

English law and Nigerian law. The chapter also provided a general overview of the legal and institutional arrangements in the Nigerian financial industry. It highlighted the problematic aspects of e-payment systems and demonstrates how the development of different payment instruments, and the involvement of different sectors in the provision and delivery of payment services impact on these arrangements. The analysis suggests that multi-stakeholder engagement in e-payment services is likely to promote regulatory conflicts and arbitrage and have far reaching implications for the overall security of the systems. The chapter further draws the inference that the advantages of convenience, innovations and development offered by e-payment systems are rivalled by the disadvantages of insecurity and crime. The analysis in chapter three identifies and examines the main ways in which cybercrime threaten e-payment systems.

Chapter Three

Cybercrime Threats to E-payment systems

Introduction

Payment institutions and payment instruments often require internet connection to initiate and complete banking and payment transactions. As was highlighted in chapter two, e-payments aggravate regulatory problems because of their multi-stakeholders' provider nature and the interconnection and interdependence between institutions directly or indirectly involved in the systems. It is further argued in this chapter that crimes on e-payment systems are dependent on the ability of criminals to extract and misuse personal information processed by the provider institutions. The chapter therefore provides an in-depth examination of the processes for exploiting e-payment systems in Nigeria particularly at the level of organisations.

The chapter starts with an exposition of the challenges of fraud reporting and how these contribute to undermining the threats posed by cybercrime to e-payments in Nigeria. It then maps the threat landscape by considering the threats posed by hacking, phishing and malware propagation. The chapter follows with an examination of how these activities potentially compromise identity information and lead to identity related cybercrimes. The chapter concludes with an assessment of how the financial industry in Nigeria has responded to the threats of cybercrime and the extent to which the responses conform to recommended information security standards in the payment industry.

3.1 Internet Fraud in Nigeria

Fraud was already an endemic problem in Nigeria before the widespread use of computer systems. However, the use of electronic systems was widely acknowledged as a great facilitator of the crime. Using computers and the accessibility enabled by the internet, fraudsters send spam mails typically requesting assistance to transfer some illegally sourced funds or legacy to bank accounts abroad. Perhaps on account of limited infrastructure for electronic money transfers and the stigmatisation of the Nigerian political class as highly corrupt, these mails appear credible and were particularly successful with foreigner victims.[1] The scale of the problem was such that the then former US secretary of state, Colin Powell

[1] See eg Harvey Glickman, 'The Nigerian "419" Advance Fee Scam: Prank or Peril? (2005) 39(3) Canadian Journal of African Studies 460.

was quoted to have referred to Nigeria as 'a nation of scammers.'[2] While sweeping statements such as this have been contested,[3] much international suspicions continue to trail activities of Nigerians on the internet whether social or commercial.[4]

Nevertheless, the adoption of e-payment systems tilted the threat landscape significantly. In terms of prospective victims, and the methods and schemes for internet crimes, targets have become more domestic and schemes have evolved to match the increasing population online. In other words, cybercrime hitherto seen as a crime targeting foreigners has become both a domestic as well as an international concern. The significance of this development was first seen in the widespread fraud associated with Automatic Teller machines.[5] In order to reduce the incidence of ATM frauds, the Central Bank of Nigeria (CBN) mandated all banks and card issuers to migrate from magnetic stripe cards to EMV cards, also called Chip and PIN cards.[6] According to the CBN, the use of Chip and PIN cards has led to the reduction of fraud on ATMs by 99% because the cards integrate technologies that make it difficult to forge or clone them.[7] However, the CBN itself admitted that fraud has migrated to other platforms particularly Card Not Present (CNP) transactions and other web based payment applications.[8] More specifically, reports on fraud and forgeries in the Nigerian financial industry through 2009 to 2012 identified 'computer fraud' or 'cyber-fraud' as the leading cause of losses to financial institutions.[9] According to the report, computer fraud represents 52.47 per cent of total amount lost to fraud and forgeries in 2012.[10] The Nigerian Electronic fraud Forum (NEFF) attributed 70% of all known cases of electronic fraud to phishing

---

[2] Howard W French, ':://www.nytimes.com/1995/10/20/world/the-leader-of-nigeria-is-elusive.html> Leader of Nigeria is Elusive' *The New York Times* (New York 20 October 1995) <http accessed 20/09/2013.

[3] See eg Olumide Longe and Adenike Osofisan, 'On the Origin of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers' (2011) 3(1) The African Journal of Information Systems 17.

[4] Eg PayPal for sometime denied registration to users traced to a Nigerian IP address and only recently included Nigeria on the list of countries and regions it supports' see 'Countries and Regions supported by PayPal' <https://developer.paypal.com/webapps/developer/docs/classic/api/country_codes/ > accessed 21/05/2014.

[5] See previous notes in 2.3.4.2 Payment Channels - Online and Offline Systems p 32.

[6] See Item 1.4.2(c) CBN E-banking Guidelines 2003.

[7] See Nigeria Electronic Fraud Forum (NeFF) Annual Report 2012. (No further reference could be provided for the report. Although, a copy was given to the researcher for the purpose of the research, it is unclear whether it was subsequently published or made available.)

[8] ibid.

[9] Financial Institutions Training Centre (FITC), 'Report on Fraud and Forgeries 2012' <https://www.fitc-ng.com/fitc_research/publications.asp.> accessed 14/10/2013.

[10] ibid.

scams.[11] The reasons for the shift to CNP transactions include the ubiquity of the internet and increasing payment mobility in Nigeria.

3.2 The Challenges of Fraud Reporting

In spite of the statistics above, there are indications that much of the published figures represent a mere fraction of the threats posed to e-payment systems. Banking regulations require banks to report cases of frauds and forgeries relating to e-banking and to highlight such reports on the returns on frauds and forgeries made to the Central Bank.[12] However, evidence suggests that gross under-reporting of fraud meant that such returns are unreliable as a source of statistics. For example, the Nigerian financial market has been described as 'a market where fraud information is kept top secret'.[13] As noted in the NEFF Annual Report, this secrecy not only impugns the integrity of fraud records but also aids criminality. In other words, because criminals are fairly certain that victim organisations are unlikely to publicise attacks or report fraud incidences to regulatory authorities, they (the criminals) leverage the situation to attack the banks one after the other using the same fraud type. This also leads to a situation where fraudsters in the markets need not be innovative and only propagate in an already fertile market.[14]

The main explanation identified as contributing to industry's propensity to keep fraud information secret ("culture of secrecy") is underlying reputational concerns surrounding organisations' fraud reporting.[15] As a report by the United Nations Office on Drugs and Crime (UNODC) also notes, underreporting of cybercrimes generally, derives from victim shame and embarrassment, and perceived reputation risks for corporations.[16] In the particular case of Nigeria, it can be argued that competition for larger market share of e-payment services may further contribute to this. For example, because it is relatively new, the market for e-payment services is highly competitive and operators struggle for dominance by consistently developing and marketing different payment solutions to both customers and non-customers. It is therefore safe to assume that to preserve the reputation of their brands, there would be less willingness on the part of providers to admit that fraud occurs or is pervasive on their payment platforms or networks.

---

[11] NeFF (n 7).
[12] See item 4.3 (b) CBN Guidelines on Electronic Banking 2003.
[13] NeFF (n 7) 6.
[14] ibid.
[15] Regulator 2.
[16] UNODC Draft Comprehensive Cybercrime Report (Draft February 2013) xxi, <http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf> accessed 22/05/2014.

Also specific to Nigeria, it can be argued that the terminologies used to describe crimes connected to computers create further barriers to effective reporting. For example, there are instances where organisations will admit that they have experienced incidences of computer crime or computer fraud but have not been victims of cybercrimes.[17] On the one hand, the perceptions and understandings of computer crimes tend to be of crimes committed by insiders such as employees who misuse passwords or exceed authorised access.[18] Usually, computer crimes can be dealt with by applying organisations' disciplinary procedures including dismissal of the guilty insider/employee.[19] Cybercrimes on the other hand are those crimes committed by outsiders such as hackers and phishers who use exploit software to infiltrate or remotely gain access to information systems.[20] To further highlight the distinctions, a policy maker argued that connectivity to the internet is a requirement of cybercrime while computer crimes can be committed on standalone computers and within closed systems.[21]

In practice therefore, distinctions are made between malicious misuse which are identified as computer crime or insider fraud and unauthorised access which is often explained as outsider fraud or cybercrime. Although, the distinctions go beyond mere semantics, they are generally unhelpful. As will be argued later in chapter four, pervasive and ubiquitous computing has undermined continued differentiation between computer and cybercrimes.[22] Nevertheless, the significant point to note here is that even when available, statistics may be misleading because computer crimes would be classified differently to cybercrimes. This puts into perspective the fact that statistics on cybercrime in Nigeria is incomplete and unreliable. It also underlines the assumption that the scale of cybercrime is perhaps broader than any reporting or empirical work could capture.

3.3 Identity Related Cybercrimes

It has been aptly noted that value in cyberspace is attached to information. Therefore, the focus of cybercriminals is the acquisition of information in order to extract its value.[23] In the context of e-payment systems, the value attached to information is money or money's worth.

---

[17] Payment service provider 2, 3, and 4.
[18] Payment service provider 2 and 3.
[19] Payment service provider 4.
[20] Payment service provider 2, 3 and 4.
[21] Policy maker 1.
[22] See further notes in 4.1.1 (Not) Defining Cybercrime p 88.
[23] See David S Wall, Cybercrime: *The Transformation of Crime in the Information Age* (Polity Press 2007) 36.

Before examining the different means by which criminals access information used for identity crimes, it is relevant to consider the concept of identity.

3.3.1 What is (Digital) Identity?

Identity is a complex concept because there are different and multiple identities serving numerous social contexts.[24] There are also different dimensions and perspectives on identity and identities have been analysed from personal, social, legal and historical and philosophical perspectives.[25] Hence we may speak of personal, legal and cultural identities as well as national, religious and gender identities. Developments in information technology have also led to the recognition of online or virtual or digital identities. Considering its scope, a discussion of the broad concept of identity may be endless and sterile in the context of this thesis. However, in order to understand the forms of identity at risk in identity-related cybercrimes, the notions of identity, digital identity and identification are considered.

The term 'identity' is not defined by law or policy in Nigeria. Generally however, identity is understood as the condition or fact of being some specific person or the condition of being the same as someone assumed, described or claimed.[26] Identity therefore means sameness or oneness as against similar or alike. A person's identity is composed of information which relates to him and singles him out from a general population.[27] For transactional purposes in the real world or offline, identity is often defined from individual, social, and legal perspectives. At the level of the individual, the concept of identity refers to the unique features, attributes and characteristics that distinguish a person. It may be established through personal or physical attributes such as appearance, facial or voice recognition or permanent attributes such as a person's DNA code. Socially constructed and legal identities are established by social or legal attributes assigned to a person by the society or the law or state. These include a person's name, address, and other identity credentials such as birth certificate, driver's licence and international passports issued by the state. Identification is the process of determining who a person is usually through one or a combination of individual, social and legal attributes. Identification is therefore the process of associating

---

[24] Emily Finch, 'The Problem of Stolen Identity and the Internet' in Yvonne Jewkes (ed) *Crime Online* (Willan 2007) 29.

[25] See eg Luciano Floridi, 'The Informational Nature of Personal Identity' (2011) 21 Minds & Machines 549; see also Samuel Warren and Louis Brandeis, The Right to Privacy (1890) Harvard Law Review 193.

[26] Kurt M. Sanders and Bruce Zucker, 'Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act' (1999) 13(1) International Review of Law, Computers & Technology.

[27] Clare Sullivan, 'Digital Identity and Mistake' (2012) 20(3) International Journal of Law and Information Technology 223.

one or more attributes with a person in order to define that person to the level sufficient for the contemplated purpose.[28] It differs from authentication which is the process of verifying or ascertaining an individual's identity.[29]

It is notable that while physical attributes and identity credentials are often sufficient to verify identities within the confines of physical environments, they become less reliable in the context of remote and distanced transactions online.[30] According to Clarke, in the context of information systems, identification involves linking a stream of data with an individual.[31] Human identification is therefore the association of data with a particular human being.[32] Such data associated with humans constitute their digitals identities. Implying correctly that individuals as well as devices can possess digital identity,[33] Cameron defines digital identity as a set of claims made by one digital subject about itself or about another digital subject.[34] Also, following this notion of identity, the OECD observed that as it relates to natural persons, digital identity involves the use of electronic identifiers by individuals in their interaction with information systems through a digital network such as the internet.[35] A person's digital identity would therefore include transactional information such as credit and debit card details as well as relational information such as usernames and passwords.[36] Therefore, in the context of electronic means of payment, usernames, passwords, and personal identification numbers (PINs) or biometric templates generated or assigned to users at enrolment will constitute part of their identity information. If tokens such as payment cards are issued, primary account numbers (PAN), card verification code (CVV), and personal identification numbers (PINs) will also form part of the identity information.

---

[28] Thomas J Smedinghoff, 'Introduction to Online Identity Management' 4 <http://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_-_Introduction_to_Identity_Management.pdf> accessed 21/07/2012.
[29] See notes on Authenticating Technologies below.
[30] See eg Roger Clarke, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7(4) Information Technology and People.
[31] ibid 6.
[32] ibid.
[33] For example, an internet protocol or IP address represents a computer's digital identity.
[34] Kim Cameron, 'The Laws of Identity'<https://msdn.microsoft.com/en-us/library/ms996456(d=printer).aspx#lawsofiden_topic3> accessed 21/02/2015
[35] OECD, 'Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy Guidance for Government Policy Makers' (OECD Digital Economy Papers 186 2011) 3, <http://www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en>accessed 15/03/2014.
[36] See eg Sullivan, (n 27).

From the perspectives of identity-related cybercrimes, digital identities can be problematic. The first problematic aspect relates to the tendency to separate digital identities from real world identities. For example, digital identities often have no direct reference to the individual using them and may be changed, revoked or discarded at the will of the user or a service provider. The identities can also be multiple and transient and may be anonymised or pseudonymised to achieve further disconnection with a person's real world identity. Accordingly, the notion of a separate digital self and digital citizenship have been advanced and promoted in recent discourse of digital identities.[37] However, it is arguable that differentiating offline and digital identities not only tend to over-simplify the problems of identity but also serve limited analytical purposes when conceptualising identity-related cybercrimes.[38] Apart from the fact that digital identities can relate to real world identities, new technologies also integrate and interlock real and digital identities across multiple domains making separation or differentiation between the identities difficult. For example, data which is anonymised or pseudonmyised for identity purposes may be de-anonymised or de-pseudonymised.[39] For the purpose of criminal exploitation of identities therefore, the increasing links between offline and online identities makes identity theft and fraud easier.

The smart card based national e-identity card proposed in Nigeria is a classic example in this respect. The card is proposed as a multi-purpose national identity card to be used for offline and online identification purposes. It embeds all identity information of the holder including unique biometric information. It is also expected to serve as an authentication token for banking and payment systems.[40] However, as a token, the identity card can be stolen. As a means of verifying identities, it could be compromised since online authentication processes can generally be defeated.[41] Criminals can also subvert the national identity database, which stores the identity information, for identity theft and fraud.[42] It is therefore arguable that access to the card or information on the card means that a fraudster can build complete or composite identity profile of a victim or use the card for both online and offline identity crimes. As stated in a Report on Identities in the UK;

---

[37] See eg 'The 2014 CLSR-LSPI Lisbon Seminar on 'The Digital Citizen'- Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15-17 October 2014' (2015) 31 Computer Law & Security Review 163.
[38] See eg Angel Adrian, 'No One Knows you are a Dog: Identity and Reputation in Virtual Worlds' (2008) 24 Computer Law and security Report 366.
[39]See eg Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques* (WP 216 10 April 2014) 4.
[40] See ss 27, 28, 29 Nigerian Identity Management Commission Act (NIMCA) 2007.
[41] See notes on Authenticating Technologies below.
[42] See notes in 5.4.3 Challenges of Identity Management p 169.

> Creating a false identity or stealing another person's identity is often achieved through obtaining key personal information, so the distinction between a person's 'identity' (in terms of their overall sense of self) and the identification used to distinguish between people online is being increasingly blurred in practice. Ultimately, stealing sufficient information could enable a criminal to effectively take over victims' online identities.[43]

The examples highlighted above suggest that even if it was possible in theory to differentiate between real world and digital identities, malicious actors and technologies considerably limit the extent to which we may do so. Therefore, it is more useful to think of digital identities the same way we think of the notion of identity generally. Correspondingly, if identity is correctly the sum total of the characteristics which determine who a person is,[44] then digital identity should be the composite or totality of information about an individual. For the purposes of further analysis in the thesis, the relevant point here is that personal information requires protection irrespective of the nature of the information and the organisation collecting it.

The second problematic aspect of digital identities concerns their legal status. It will be argued later in the thesis that it is challenging to determine whether generally, identities or identity information are capable of being stolen under the law. It will also be argued that the protection of identity information is linked to the more restrictive legal concept of 'personal information'. Therefore, it is the law which defines specific information as linked or linkable to an individual for protection purposes. For the purposes of further analysis in this chapter, it suffices to state that identity crimes generally refer to the misuse of another's personal or identifying information. From the perspectives of information systems, identity-related crimes are committed by defeating the verification or authentication strategies of a networked system. This enables a person to identify himself as someone else. Depending on the nature of the transaction, circumventing authentication processes may enable the identity criminal to access benefits to which he is not otherwise entitled or to avoid detriments to which he would otherwise be subject.[45] Invariably, identity/personal information is at rsisk of theft when criminals compromise proprietary systems of service provider organisations.

---

[43] Government Office for Science, *Foresight Future Identities Final Project Report 2013*, 4 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273966/13-523-future-identities-changing-identities-report.pdf.> accessed 12/04/2015.
[44] ibid 3.
[45] Russell G Smith, 'Biometric Solution to Identity-related Cybercrime' in Yvonne Jewkes, (ed) *Crime Online* (Willan Publishing 2007) 44, 45.

The following sections explore the vectors or means through which criminals' access and exploit identity information in e-payment systems.

3.3.2 Threat Vectors and Activities

As the common denominator for the provision of e-payment services, the internet provides access to both legitimate and illegitimate users. Therefore, the main vectors of criminal attack on e-payment systems correspond to the payment channels, instruments and institutions analysed in chapter two. These would include the databases and websites of banking and non-banking e-payment service providers as well as e-commerce sites. They would also include payment channels such as ATMS and POS terminals. For example, payment terminals and websites are attractive to criminals because they provide a viable source of harvesting personal financial information such as PANs, PINs, CVVs and usernames and passwords. Databases are also attractive because of the large amount of personal information accessible through the source. E-commerce sites provide the platform both for harvesting and for the use of fraudulently sourced or stolen account and payment details. The common threat actions identified include hacking or unauthorised access into information systems, and phishing, and malware propagation. For organisations, these threats increase the risks of data breaches and the possibilities of identity related crimes.

3.3.2.1 Hacking (Unauthorised/Illegal Access to computer Systems)

Hacking refers to unauthorised intrusion, disruption, manipulation and exploration of a computer system. It involves attacks against the availability, confidentiality and integrity of computer systems and data. Hackers illegally access computer systems to explore and/or steal information.[46] Although hackers attack individual and standalone systems, for payment systems, the main threats posed by hacking lays in the possibility of hackers compromising customer information in custodian systems such as banks' and other payment service providers databases. Such compromise may entail breach of confidentiality or theft of personal and financial information. For example, hackers can manipulate web applications to make fraudulent transfers from compromised accounts to accounts under the control of the hacker. Apart from stealing data, hackers can also generally compromise websites to leverage further damaging attacks such as to propagate malware or launch denial of service (DoS) or phishing attacks.[47]

---

[46] Douglas Thomas and Brian D Loader (eds) *Cybercrime Law Enforcement Security and Surveillance in the Information Age* (Routledge 2000) 6.

[47] For example, as a symbol of protest, the website of Nigerian electoral body, the Independent National Electoral Commission (INEC) was hacked by a group identifying

Technical security experts in Nigeria estimate that over 3000 'maliciously crafted attacks' are directed at payment service operators every day.[48] However, evidence suggests that hacking is still more of a perceived than an actual threat in the industry. It was argued for example that 'Nigerian hackers' are made up mainly of "hacktivists" or cyber-activist often motivated by political agenda of correcting perceived inequalities and injustice.[49] Correspondingly, the main targets of the "hacktivists" are websites belonging to government and its agencies.[50] These explanations carry an underlying assumption that hackers are less likely to attack private or financial organisations because their (hackers') motivations are seldom financial.

It was also argued that since financial databases and information systems are often more secure than those of government organisations, hackers are unlikely to succeed even if they attack financial systems. In effect, hackers lack the technical skill and knowledge to defeat the up-to date and robust technical security of the financial industry making financial information generally less accessible to criminals.[51] Summed up as a simple argument, service providers' views are that hackers are more active in the political rather than the financial arena, and that both the robustness of security and the low technical skills of the hackers have reduced the possibilities and potency of cyber-attacks. Invariably, this accounts for why there does not seem to be reports of hacking and data breaches or data theft incidents in the Nigerian financial industry.

If one accepts these explanations as mirroring the position of industry, then, it must also be assumed that any proposal to control the threats of hacking is speculative and premature. However, this assumption is not supported by the literature or empirical evidence. The data suggests that the crimes are being contested and acknowledged at the same time. For example, it was contended that cybercrimes are not presently a problem for law enforcement in Nigeria because the crimes are not very pervasive.[52] At the same time, the observation was made that 'The integrity of the payment systems is at stake unless we do something about controlling cybercrimes'.[53] Furthermore, measures taken by the financial industry suggest haste, if not desperation, to counter e-payment fraud. The establishment of the

---

itself as the Nigerian Cyber Army Team NCA in the wake of the March 2015 general elections.

[48] IT security expert 1.

[49] Payment service providers 2, 3 and 4.

[50] Payment service provider 2 and 3.

[51] Payment service providers 1, 2, 3, 4, 6.

[52] Law enforcement 1.

[53] ibid.

Nigeria Electronic Fraud Forum (NeFF),[54] and introduction of the Bank verification number (BVN),[55] are examples which point at attempts to find a solution to problems which by industry assessment are 'non-existent'.

As analysis earlier in the chapter suggests, a better explanation is that because it raises reputational concerns, organisations would not readily admit that their systems have been hacked. Moreover, as argued by a service provider, an organisation's obligation is limited to reporting fraud and not "mere threats". [56] "Mere threats" in this instance refers to security breaches resulting from hacker infiltration. This observation appears to suggest that unless a breach of security leads to fraud, then service provider organisations are not obliged to comply with reporting obligations. If the clear, albeit technical distinctions between a data breach and a security breach is applied, this observation would be correct. A data breach is a type of security breach which involves the release or loss of personal information which can be used for identity-related crimes. Other security breaches may not lead to such losses. For example, a security breach may include defacement of websites, hacktivism, or distributed denial of service (DDoS) which do not necessarily involve the theft or compromise of personal information.[57] In practice therefore, a data breach would be a security breach but a security breach will not necessarily lead to a breach of data or loss of personal or identifying information. In effect, the observation must be taken as implying that data and security breaches do occur, but are not reported unless fraud also occurs. It must also be taken to imply that since there is no regulatory or statutory reporting requirement for data breaches, organisations are justified to deal with data breaches as internal security problems.

While the notion of data or security breaches may be technical and contestable, the perceptions of hackers and their motives are less correct. As noted above, assumptions are made that hackers can be categorised according to their intent and they generally lack the skills to infiltrate more secure systems and networks. The literature suggests that these assumptions are mistaken and incorrect. Gragido et al argue for example that although

---

[54] The Neff was set up as an alternative forum for fraud reporting on account of limited success of the Central Bank of Nigeria to compel banks and other non-bank financial institutions to report fraud.

[55] The BVN involves enrolment and use of bank customers' biometric information for banking and payment transactions; see further notes in 5.1.3 CBN Bank Verification Number (BVN) p 139.

[56] Payment service provider 7.

[57] See eg Ponemon Institute, 'The Post Breach Boom' (2013) Ponemon Institute Research Report<http://www.ponemon.org/local/upload/file/Post%20Breach%20Boom%20V7.pdf>accessed 27/04/2015.

hackers are traditionally categorised as insurgents, this characterisation has changed in the contemporary context. As they observe;

> Previous books on hackers and hacking tended to get weighed down by the personality traits of hackers—depicting mainly male, acne-faced teens and young adults dressed in black and perpetrating their crimes in black-lit rooms of various types … Hackers who face large corporations are typically well financed, are organized, and have analysed the saleability of the information they pilfer.[58]

Contrary to arguments typifying hackers and their attacks therefore, the point here is that hackers could be highly skilled and could potentially attack any organisation. However, even if one concedes, for the purpose of argument, that financial organisations, such as banks are secure from hackers, this does not lead to the invariable conclusion that information which may be targeted for fraudulent use is secure. As demonstrated in chapter two, multiple organisations, including non-bank e-payment service organisations, now collect and store personal information. Therefore, any system could be compromised and personal information thereby accessed used for fraud. To state the point differently, even if hackers target non-financial databases, it is incorrect and misleading to conclude that they have non-financial motives or that they pose no threats to financial information. To further support this point, research indicates that hackers have become notoriously erratic as their attacks fail to follow any logical sequence of whether or not victims have money or valuable information. Accordingly, since hackers are unpredictable, organisations should be doubly concerned.[59]

Moreover, since criminals are also likely to hack information systems of smaller or non-financial organisations and even individual devises of users, these may provide alternative access into systems and networks of larger (financial) organisations. Mobile payments for example are capable of providing access points to information held in banks' databases. They may also enable attacks on telecom companies using mobile devices as gateway for electronic payments.[60] Available statistics show that some of the largest data breaches have involved not only banks or other financial institutions but also retailers. For example data

---

[58]Will Gragido et al, *Blackhatonomics an Inside Look at the Economics of Cybercrime* (Elsevier 2012) 3-4.
[59] Verizon 2012 Data Breach Investigation Report (DBIR) <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf accessed> 15/05/2013.
[60]See Symantec, *Internet Security Threat Report* (ISTR) Vol 17 April 2012, 25.

breaches at TJX in the United States indicate that any organisation within the payment system is susceptible to attacks and hackers would exploit the weakest and most vulnerable link in the payment chain. Therefore, bigger organisations could suffer direct losses and collateral losses as a result of data breaches in smaller organisations.[61] According to the Verizon 2015 PCI Compliance Report, no country, industry, or company is safe from cybercrime.[62] As Newman and Clarke also rightly observed;

> …as far as the internet is concerned, any business that is connected to it is at risk of criminal attack, even if that business is not directly or even specifically the target of the criminal. Since information has become the key ingredient in e-commerce…all e-commerce becomes a target.[63]

Finally, it is arguable that the availability of crime statistics in the context of cybercrimes is tied to the ability to detect the threats and data breaches in the first place. In other words, assumptions that financial systems have not been compromised may actually be indicative of non-detection rather than the absence of threats or breaches. As later analysis in the thesis demonstrate, the likelihood of detection further diminishes where there is a dearth of forensic investigative skills as appears to be the case in Nigeria.[64] Overall therefore, although it is difficult to establish the pervasiveness of hacking as a threat to new e-payment systems in Nigeria, alternative explanations demonstrate that this cannot be taken as absence of this threat.

3.3.2.2 Phishing

Phishing refers to fraudulently obtaining financial information from the victim, typically through the use of e-mail and spoofed sites.[65] The Anti-phishing Working Group (APWG) identifies two forms of phishing attacks. The first involves the use of social engineering

---

[61] Eg in the TJX cases, affected banks were reported to have incurred costs of over $1 billion to replace compromised cards, see Stacy L Schreft, 'Risks of Identity Theft: Can the Market Protect the payment System' (2007) Economic Review Fourth Quarter Federal Reserve Bank of Kansas City.

[62] Verizon, 'Verizon 2015 PCI Compliance Report Insight for Helping Businesses Manage Risk through Payment Security' 4. <http://www.verizonenterprise.com/placeholder/resources/reports/rp_pci-report-2015_en_xg.pdf accessed 13/05/2015.

[63] Graeme R Newman and Ronald V Clarke, *Superhighway Robbery: Preventing E-commerce Crimes* (Routledge 2003) 46.

[64] See notes in 4.6.1 Lack of Computer Forensics Capacity in Law Enforcement p 130.

[65] Kenneth C Laudon Carol and Guercio Traver, *E-Commerce 2011 Business Technology Society* (7th edn Pearson 2011).

methods and the second the use of technical subterfuge or pharming.[66] In social engineering or e-mail based attacks, the phishing scam involves three phases. In the first phase, the criminals identify legitimate organisations offering electronic services such as online banking. They then design spoofed sites which are similar or look-alike websites of the legitimate business. The second phase involves sending out e-mails (called spammed e-mails) similar to those of the legitimate organisations. Generally spam is understood to mean unsolicited and unwanted electronic messages. However, the OECD includes the word 'harmful' in its definition because spam is increasingly being viewed as a vector for malware and phishing scams.[67] The spam mails will usually request users to provide personal details such as passwords, PINs or other identifying information. In the third phase, the scammers use the information supplied to log into the victims account and to unlawfully transfer money or commit other identity-related offences.[68]

In contrast, pharming or malware based attacks employ a technical method using malware installed on username or Domain Name Server (DNS) or embedded in spam mails. The malware automatically re-directs users to the spoofed site whenever they attempt to access legitimate services such as electronic banking. It then prompts the users to enter personal log on information which is subsequently used for identity fraud.[69] Malware based methods are also used to perpetrate man- in -the -middle attacks, an attack which enables the phisher using designated malware, to intercept messages or instructions intended for legitimate businesses or organisations. [70]

Phishing scams are blended and adjusted to new technologies in payment systems and are increasingly able to target both individuals and institutions. More significantly, payment services and the financial sector are the most targeted sectors for phishing scams.[71] Although not clearly defined in Nigeria, phishing is conceived as the use of technology to perpetrate deceit and is said to account for an estimated 70 per cent of fraud in e-payment

---

[66] Anti-Phishing Working Group (APWG), Phishing Activity Trends Report, 3rd Quarter 2014 <http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf.> accessed 09/04/2015.

[67] OECD defines spam as unsolicited, unwanted and harmful electronic messages; see OECD, 'Policy Guidance on Online Identity Theft' (OECD Ministerial Meeting on the Future of the Internet 17-18 June 2008) 3<http://www.oecd.org/sti/consumer/40879136.pdf accessed> 12/09/2013.

[68] ibid.

[69] UNODC, *The Globalisation of Crime: A Transnational Organised Crime Threat Assessment* (UNODC 2010) 204.

[70] See further notes below at p 82.

[71] See Anti-Phishing Working Group (APWG) Phishing Activity Trends Report (n 66) 7.

systems.[72] Phishing activities in Nigeria are generally correlated to the APWG classification into socially engineered phishing methods using fraudulent e-mails and malware based phishing. Citing specific examples, the following sections demonstrate the pattern and trends of phishing scams in Nigeria.

(a) Spam mails

Spam mails used to perpetrate fraud on e-payment systems often request recipients to update their account details by following a clickable link to their bank or other organisation's website. Payment service providers in Nigeria confirm the rising incidents of spam and the fact that in spite of aggressive user awareness initiatives, many consumers continue to fall for the scam.[73] However, it can also be argued that the response rate to scam mails is increasing because of the innovativeness and creativeness of criminals in constructing believable mails which mirror those sent by organisations to their customers. The examples in tables 3.1 and 3.2 depict such scam mails.

Dear Valued Customer, As part of our continuous efforts towards providing you with excellent customer service and ensuring efficiency in transaction processing, we request that you kindly update your records with the Bank by going to https://xxxbanknig.com/update//login.aspx This update will help us to prevent any unauthorised or illegal use of our customers identity and to confirm that you are truly the owner of the account you are operating. Failure to update your account now will lead to termination of your account and internet banking services for security reasons. Click here now for the update. If this message is in your spam folder kindly move the mail to your inbox to enable you click on the account update link. XXX bank is committed to protect the identity of its internet users. Help us to serve you better. It's all about your security. Thank you for choosing XXX bank.

Table 3.1 sample spam mail

Absent the tell-tale signs of bogus or fictitious mails such as grammatical and spelling errors, e-mails such as the above appear credible and can more easily convince the

[72] See NeFF Annual Report 2012.
[73] Payment Service provider 1, 2, 3, 4, 5, 7.

recipients. Notably, scammers also exploit privacy and security concerns among users and appear to have created "scammers' diction" to match these concerns. For example new scam mails now purports to come from non-existent "privacy departments" of commercial banks. One of such 'privacy scam mails' reads as follows;

No Reply@XXXcontacts.com To Recipients, Dear XXX Bank Nigeria Customer, Notice attention to us by The CBN To Upgrade Our security, To cashless policy and enable all our customers tranzact Cashless. Kindly activate XXX Cashless Platform b www.XXXnigeria.com/cashless/XXX /XXXonline-ng/ Thank You. Privacy Department. (c) 2013 XXX Bank Nigeria

Table 3.2 – Sample privacy spam mail

(b) Spoofing

As described above, fraudulent e-mails usually contain a clickable link leading to a website identical to that of the bank which purportedly sent the e-mail. The user/victim is prompted to click on the link. However, rather than take him to the bank's legitimate site, the link takes the victim to an identical or 'spoofed' website of the bank. A spoofed site is a bogus site and once the user enters his password and account details, these are captured by the phisher and the information may be used to access the user's bank account (internet banking fraud) or to perpetrate other identity related fraud. The most common use of the information is transferring money from the victims account to an account under the control of the phisher.

(c) Domain Based Phishing

This form of phishing is close to the one described above. The main difference however is that in domain based phishing, the sites are not spoofed. The fraudster registers a domain name similar to the trademark of an organisation with only slight differences. The victim is then directed to this website rather than to the authentic site of the bank. While more computer savvy persons may detect spoofing, domain based phishing may be more difficult to identify. It is therefore a method devised to make the sites more believable and increase the chances of users falling for the scam. Generally, in Nigeria, prospective companies may

be refused registration on grounds that certain names are prohibited or infringe on existing names or trademarks.[74] However, there is no such practice for domain names registration and it has been argued that domain name spoofing is aided by the lack of effective regulation of domain name registration generally.[75]

A further challenge identified with respect to domain based phishing is associated with the regulation of Internet Service Providers (ISPS) in Nigeria. Although the Nigerian Advance Fee Fraud Act requires that all ISPs be registered with the Economic and Financial Crimes Commission (EFCC),[76] full compliance with this law is difficult to achieve. This is because some organisations use foreign ISPs and while foreign ISPs are also required to appoint agents in Nigeria and register, most of them fail to do so. The challenge then is that such ISPs cannot be regulated and it is often difficult for law enforcement agencies to solicit their assistance in shutting down offending websites.[77]

(d) Context-aware Phishing

Jakobbson describes Context-aware phishing as a form of phishing in which the attacker exploits some knowledge about the victim to enhance the efficacy of the attack.[78] In context-aware phishing, criminals depend on available information about an individual to collect additional information either from the individual himself or from other sources. Therefore, phishers can use a combination of information sourced from the internet, personal interactions, public records and physical world information to commit identity crimes online. In Nigeria, Information from social networking sites such as Facebook and professional network sites such as Linked-In were identified as particularly susceptible to exploitation for context-aware phishing.[79] Since the phisher may already have some background information such as the victim's first name, surname, mother's maiden name, e-mail, telephone number, profession or address, phishing or forged e-mails sent to the victim are personalised and more believable.[80] For example a scam e-mail to a bank customer will

---

[74] IT Security expert 1.
[75] See eg Mike Rodenbaugh, 'ICANN Policy Developments on Abusive Domain Name Registration'<http://rodenbaugh.com/downloads/pdf/IPLitigator_AbusiveDomains.pd> accessed 19/02/2013.
[76] See s 13 Advance Fee Fraud and Other Related Offences Act Cap A2 Laws of the Federation of Nigeria 2004.
[77] Law enforcement agent 1.
[78] Markus Jakobsson, 'Modelling and Preventing Phishing Attacks' <http://markus-jakobsson.com/papers/jakobsson-fc05.pdf> accessed 15/02/2014.
[79] Law enforcement 1.
[80] See notes on Spear Phishing below.

not address the victim as 'Dear Customer, rather, it may contain the victim's title and first name such as 'Dear Dr Jane Doe.'[81]

(e) Smishing/ Vishing

Vishing and smishing are not necessarily referred to by these terms in Nigeria. It is more usual to describe them simply as SMS fraud. Vishing is a combination of voice and phishing. It involves the use of social engineering over the telephone system and deploys features such as Voice over Internet Protocol (VoIP).[82] Smishing is short message service (SMS) based phishing scam which targets users of mobile phones through fraudulent text messages.[83] In a typical Nigerian smishing or SMS scam, the prospective victim is informed via SMS that he has won a lottery or has been drawn among the winners in a competition, often one that he has not entered at all. The message might also inform the prospective victim that he has won an all-expense paid holiday to an exotic location or has been chosen to receive supplies of certain products for a designated time.[84] To enable the organisation to fully process or make other arrangements to facilitate the victim's access to the winnings, holidays or products, he is advised to contact the organisers through a phone number. If the victim makes the call, he is prompted to 'confirm' his personal information including his name, address, bank account number, date of birth, mother's maiden name, place and address of workplace. He may also be asked details of his national identity card number and even information such as spouse name, and the names and age of children and even car registration number.[85] While seemingly incongruous, much of the information gathered through this process is used in context phishing (described above) to demonstrate familiarity with the victim or to build trust. This in turn could be used for other fraudulent purposes such as identity fraud involving applying for debit cards on the victim's account or for SIM swap frauds.[86]

As observed by a security expert, smishing frauds are particularly enabled by lack of data protection requirements. He contends that organisations such as MNOs are implicated in the fraud because they sell subscribers information including phone numbers for marketing purposes and for other purposes which may be unknown or undisclosed by the "information

---

[81] Law enforcement 1.
[82] See eg OECD, 'Policy Guidance on Online Identity Theft'(n 67).
[83] ibid.
[84] Law enforcement 2.
[85] ibid.
[86] See notes on Account-take Over Fraud and SIM Swap Fraud below.

buyers" at the time of the sale.[87] Furthermore, although, the scams are perceived as generally targeting users, they also victimise organisations. For example, smishing scams exploit and undermine reliance on the transaction notification system put in place by banks to check incidents of fraudulent transactions and payments. A transaction notification or 'alert' is an SMS or e-mail sent to an account holder whenever any credit (credit alert) or debit (debit alert) transaction occurs on the account. There are also "log in alerts" designed to inform users of recent logs into their accounts and advising them to change passwords or contact their service providers/banks if they did not initiate the log-in. [88] To undermine this system however, fraudsters send fraudulent SMS alerting users of e-banking or e-payment services to fictitious log-ins or transactions. The users are then advised to follow certain links or call designated numbers for assistance. Invariably links lead to spoofed sites and phone numbers are answered by fraudsters who then collect personal or identity information under the guise of providing technical or other assistance. [89]

(f) Spear Phishing

Spear phishing uses a combination of social engineering and technical subterfuge and is often successful because the phisher has obtained preliminary information about the victim as explained above. Spear phishing targets employees of an organisation rather than individual users. An e-mail purportedly from a trusted or known source within or outside the organisation is sent to the employee. The mail usually contains a link or an attachment which if clicked or opened by the employee installs malware which transmits organisational passwords to the phisher.[90] Similar to hacking, this form of phishing may lead to large scale data breaches because it provides access to information in proprietary systems. In spite of the fact that organisations can themselves be victimised by phishers, it is common for organisations simply to blame users and consumers for any form of phishing attack and thus shift fraud liabilities to unsuspecting users.[91]

Also, notwithstanding the threats to organisations, phishing scams are generally perceived as familiar frauds utilising very basic technology. As service provider 2 observes, '…phishing is very basic technology and there is nothing hi-tech about it.' Law enforcement agent 3 also argues that phishing scams threaten naïve and negligent users of information

---

[87] IT Security expert 1.
[88] See example in *Table 6.1- Sample spam login alert* p 207.
[89] Law enforcement 2.
[90] Richard G. Brody, Elizabeth Mulig and Valerie Kimball, 'Phishing, Pharming and Identity Theft' (2007) 11(3) Academy of Accounting and Financial Services, 43.
[91] IT security expert 1.

systems and presents no new challenges for the criminal law. Based on the antecedents of electronic fraud in Nigeria, the rationale for this perception is not far-fetched and easily understood. The use of deception to commit crimes in Nigeria is not new. The Nigerian mail scam popularly referred to as 419 or advance fee fraud has gained notoriety over the years for both online and offline frauds. [92] In 419 scams, the fraudsters typically bait their victims by demanding that small amounts of money (or advance fees) be transferred to them as tax, fees or charges to accelerate the release or transfer of a larger sum. The fraudsters will usually claim that the whole or part of the larger sum is the ill-gotten wealth of a corrupt politician, a disputed or unclaimed inheritance or government payment for some unexecuted public sector contracts.[93]

However, in spite of the similarities between that phishing and 419 scams, they are distinguishable in a number of ways. It can be argued for example that 419 scams operate independently of the internet and are now easily identified that fewer people fall for the scam. Also, while 419 scams tend to target victims especially in foreign countries, phishing scams focus more on e-payment service providers and e-commerce sites whether they are local or international. Phishing scams are also potentially more dangerous because they can reach a wider range of victims using more convincing form of deceit such as pharming or spear-phishing. For example, although 419 or advance fee fraud have been rated one of the highly successful criminal tactics, the mails are often characterised by tell-tale signs such as poor grammar and spelling errors which tend to make deception discernible and obvious. As a result, a common theme in research into advance fee fraud is that people fall for the scam not so much because it is convincing but more because they are motivated by greed and are themselves inclined to fraudulent or criminal behaviour.[94] In comparison, phishing scams contain well-designed copy-cat websites and logos of genuine organisations making the scams more difficult to detect. Accordingly the Microsoft Security Intelligence report 2013 observed as follows:

> Malicious websites typically appear to be completely legitimate and often provide no outward indicators of their malicious nature, even to the experienced computer user. In many cases, these websites are legitimate websites that have

---

[92] The 419 scam is named after its violation of section 419 of the Nigerian Criminal Code which creates the offence of obtaining property by false pretence.
[93] See eg Harvey Glickman, 'The Nigerian "419" Advance Fee Scams: Prank or Peril' (2005) 39(5) Canadian Journal of African Studies 460.
[94] See eg M.C Ogwezzy, 'Cybercrime and the Proliferation of Yahoo Addicts in Nigeria' (2012) 1 International Journal of Juridical Sciences 86.

been compromised by malware, SQL injection, or other techniques in an effort by attackers to take advantage of the trust users have invested in them.[95]

As a further example, it used to be possible to identify phishing sites by looking out for technical indicators which may alert a user that the website is spoofed. This includes the fact that spoofed sites are served in the bar over HTTP as opposed to HTTPS and are often hosted on IP addresses as opposed to a registered domain. As research established, these indicators are becoming less useful as spoofed sites can be served over HTTPS because they have been copied and pasted.[96] Therefore, as noted previously, phishing attacks are more sophisticated, and increasingly incorporate elements of context to become credible and effective.[97] In order to illustrate how phishing undermine the integrity of genuine websites, one service provider admitted that there are over 100 spoofed sites of his organisation (a bank) and the technical unit is unable to keep pace with taking them down. He argues that this gives the criminals a edge as all the organisation can do is to accelerate the pace of user awareness.[98]

Finally, it is important to mention that although both 419 and phishing scams can be linked to criminal organisations as well as lone offenders, potentially, anyone with access to the internet can purchase a phishing kit and execute an attack.[99] This considerably increases the poll of perpetrators and victims of phishing scams. As will be demonstrated in subsequent analysis in chapter four, the differences between 419 and phishing scams limit the applicability of provisions of the law dealing with fraud and deception offences in Nigeria.[100]

3.3.2.3 Malware

The activities of Hackers and phishers are facilitated by propagation of malware or malicious code or software. Malware has therefore been referred to as both a standalone

---

[95] Microsoft, *Microsoft Security intelligence Report* (vol 14 July through December 2012), 65.
[96] See Xun Dan, John A Clark and Jeremy L Jacob, 'Defending the Weakest Link: Phishing Websites detection by Analysing User Behaviours' (2010) 45(2-3) Telecommunication systems 215.
[97] See Table 3.1 and Table 3.2 above.
[98] Payment service provider 4.
110 see eg OECD, 'Policy Guidance on Online Identity Theft' (n 67).
[100] See further notes in 4.3 Phishing- Fraudulent Representation and Computer-related Fraud p 112.

cybercrime,[101] and an 'infrastructure supporting cybercrime.'[102] Malware is the use of unintentionally installed software to collect and transmit personal information on an information device. Its main purpose is to subvert a system to function in a way otherwise than that intended by the legitimate user. Methods used to propagate malware include the key loggers, Trojans, viruses and worms and bots or botnets. According to Anderson et al, botnets for example provide a versatile platform for a variety of criminal business models. They can be used to send spam messages, to commit click fraud, harvest accounting details and credentials, and for phishing. Targeting botnets at organisations can also result in denial of service attacks which can deny users' access or ultimately bring down the website.[103] Malware constitute substantial threats to e-payments generally. For example, in 2007, the Estonia's government was forced to shut down government and financial institutions following a coordinated attack by over one million computers worldwide which have been organised into a botnet.[104] Also, in 2014, the malware Gameover Zeus (or GoZeus) which steals financial information such as online banking details was identified as the most sophisticated spyware so far.[105]

A report by Microsoft suggests that malware constitutes a significant threat to computers and networks in Nigeria. As at 2012, the report indicated that malware was detected on 7.0 of every 1,000 computers scanned in Nigeria.[106] This represents a score of 7.0 computers cleaned per 1000 scanned (CCM) compared to a worldwide average CCM of 6.0.[107] More recent reports also suggest that malware propagation is still relatively high in Nigeria.[108] In addition, the use of smartphones and other mobile devices with connectivity to the internet, as well as the development of mobile applications in Nigeria provide a fertile environment

---

[101] See OECD, Anti-spam Toolkit of Recommended Polices and Measures (OECD Publishing 2006).
[102]Ross Anderson et al, 'Measuring the Cost of Cybercrime' (2012) 19 <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf> accessed 03/08/2012.
[103] ibid.
[104] See eg Clay Wilson, 'Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress' (Congressional Research Service 2008) <http://www.fas.org/sgp/crs/terror/RL32114.pdf> accessed 02/09/2013.
[105] See FBI, 'U.S. Leads Multi-National Action against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator' <http://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator> accessed 01/07/2014.
[106] see Microsoft Security Intelligence Report Vol 14 2012.
[107] ibid.
[108] See Microsoft Security Intelligence Report vol 17 2014.

for malware infection.[109] Mobile applications are particularly vulnerable because there is generally lack of verification for mobile software and traditional security controls such as firewalls and encryption are not sufficiently optimised for mobile devices.[110] Therefore, because it increases the possibility of users installing unregistered third party applications, mobile devices also increase the potential victim pool for malicious code writers.

3.4 Criminal Misuse of Identity Information

The foregoing analysis demonstrates that the activities of cybercriminals compromise the integrity of data. Although, this compromise, often referred to as data breaches, may also be due to accidents, errors, or negligence,[111] in the particular case of corporate and proprietary systems, criminal compromise caused by hacking, phishing and malware may precipitate data breaches. However, malicious breach of data is seldom an end in itself, and in e-payment systems, stolen or compromised identity information may be used in three main ways. The first is using the information to commit fraud on existing accounts, also called existing account fraud. This type of fraud involves the fraudster using stolen identity information to gain access into or control over the victim's existing bank account or payment cards. The second fraud, referred to as new account fraud involves the use of stolen or compromised identity to open new accounts or new lines of credit in the victim's name. In the third variant of the fraud, the fraudster combines stolen identity information with identity information relating to a fictitious or non-existent person to form a new or synthetic identity.[112] In Nigeria, account-takeover fraud is the most pervasive.[113] They manifest majorly as account/card fraud, Card not present transaction fraud, internet banking fraud and SIM swap fraud.

3.4.1 Account Takeover Fraud

Account take-over fraud involves impersonating an account holder in order to make fraudulent transfers, or payments or withdrawals from the account. A typical account takeover fraud involves a fraudster applying for a debit card on another person's account. A payment service provider cites an example of an instance where after "due verification" his bank issued a debit card to a fraudster under the belief it was dealing with the authentic

---

[109] For the statistics on mobile phone subscription, see (n 83) at p 33.
[110] See (n 84) at p 33.
[111] These are unintentional breaches caused by insiders, third party security companies and so on and are often referred to as non-malicious data breaches.
[112] Stacey L. Schreft, 'Risks of Identity theft: Can the Market Protect the Payment System? (2007) Federal Reserve Bank of Kansas City Economic Review Fourth Quarterly 5.
[113] Law enforcement 1, 2.

account holder.[114] According to the provider, the whole transaction was unknown to the genuine account holder until the fraudster used the card to make purchases at a point of sale. Notably, the provider argues that the loss was minimised by the fact that only a single fraudulent payment is possible on the account because of the transaction notification system put in place by the bank.[115] However, the fraudster knowing this makes a single but large purchase up to the limit allowed on the card. On receiving a transaction notification, (or debit alert) of an unfamiliar and large transaction, the account holder had contacted the bank.

The only indicator of fraud, as stated by the service provider, is the fact that the fraudster applied for the card outside the State in which the account was domiciled. However, in spite of this indicator, the bank declined to indemnify the account holder. The bank had argued that refund would only be made to the account holder subject to the bank establishing to its (the bank's) satisfaction that the customer was not complicit in the fraud. It is relevant to note that most service providers confirm that their organisations will take the same approach to a refund in similar circumstances.[116] In addition to raising questions about identity management, this example has implications for allocation of liability in contested and fraudulent payments.

3.4.2 Internet Banking Fraud

Internet banking fraud is a form of account-takeover fraud. It is perpetrated when fraudsters have obtained a customer's identity information such as accounts and authentication details using hacking, phishing scams or malware based attacks. The fraudster uses the information to gain access into online banking services often to make fraudulent transfers or payments into accounts or payment cards under the control of the fraudster. The commission of internet banking fraud is particularly aided by the use of ATMs and prepaid cards. To make tracing and detection more difficult for example, the fraudster (often acting in conjunction with others) immediately collects the proceeds of the crime from ATMs using prepaid cards.[117] According to law enforcement 2, the process of collecting criminal proceeds through ATMs make trailing and arrest of criminals difficult because prepaid cards can be obtained under fictitious names in spite of industry's Kow Your Customer (KYC) requirements. Also, similar to account takeover fraud, liability for internet fraud is displaced by bankers and other service providers' insistence that account holders were negligent, fraudulent or collusive.

---

[114] Payment service provider 6.
[115] See notes on transaction notifications at p 66 .
[116] Payment Service Providers 1, 2,4,5,6, 8.
[117] Law enforcement agent 2.

3.4.3 Card Not Present Transaction Fraud

Card not present transactions fraud involves the theft of genuine card details that are then used to make purchases over the internet, by telephone or by mail order.[118] The most frequently perpetrated fraud is on e-commerce sites particularly the websites of local and international airlines. Typically, fraudsters have acquired information through any of the methods discussed above, or have stolen a payment card or somehow obtained information on a card. Transactions for the purchase of airline tickets are initiated and the details of the cards are entered as if the owner is making the purchase.[119] Crucially, this fraud undermines the advantages gained by migration from magnetic stripe cards to chip and PIN or EMV cards mentioned above. This is because online, the security integrated into the (EMV) cards is lost as neither the chip nor the PIN is required for the fraud.

3.4.4 SIM Swap Fraud

Subscriber Identity Module or SIM swap is a fraud enabled and facilitated by both the use of mobile phones and mobile banking applications. To perpetrate the fraud, a fraudster applies for a replacement of mobile SIM cards issued to someone else. Presumably, the fraudster already has the victim's personal information including his name, address, age, occupation and other relevant information. The fraudster then lodges a report with the mobile service provider to the effect that the SIM is lost, and using the information which he has acquired, he applies for a replacement. If the SIM is replaced, the fraudster, posing as the accountholder may then download mobile banking or payment applications with respect to the account associated with the particular phone number. Often fraudsters can initiate fund transfers or make payments for goods and services using the fraudulently installed mobile banking or payment applications to intercept SIM based one time passwords (OTPs).[120] It is notable that to curb this fraud, the Nigeria Communications Commission (NCC) introduced biometric registration of telephone subscribers, however the processing of subscribers' information raise equally fundamental questions about the nature and security of identity information.[121]

---

[118] See eg Financial Fraud Action UK <http://www.financialfraudaction.org.uk/Media-cnp-fraud.asp> accessed 13/09/2013.
[119] Law enforcement agent 2.
[120] ibid.
[121] See notes in 5.1.2 NCC SIM Registration p 138.

3.5 Industry Responses to cybercrime Threats –Private Ordering and Technical Security Standards

The remaining part of this chapter analyses the responses of the financial and payment industry to the threats of cybercrime. It considers in particular the established global private ordering systems and the extent to which they have been integrated and adopted in Nigeria. The section provides important background for later analysis in the thesis on the limits of technology to control identity-related cybercrimes in e-payment systems.

3.5.1 Central Bank of Nigeria (CBN) Regulations on Privacy and Security

Industry standards for protecting privacy and security are contained in the CBN E-banking Guidelines 2003 and the CBN POS Guidelines 2011. In the case of internet banking, the e-banking guidelines require banks to put in place procedures for maintaining the banks websites. The procedures include ensuring that access is limited to authorised staff only. Banks must also ensure that updates of critical information are subject to dual verification and that website information and links to other websites are verified for accuracy and functionality. In addition, management should implement procedures to verify content, software and interactive programs available to customers on the banking website and ensure that links to external websites contain disclaimers and disclosures on the consequences of following such links. Where service is outsourced, the guidelines provide that banks have the obligation to ensure that the internet service provider (ISP) has implemented firewall to protect the banks website.[122] ISPs in turn are required to exercise due diligence to ensure that only websites of financial institutions duly licensed by the CBN are hosted on their servers. The Guidelines provide that ISPs that host unlicensed financial institutions would be liable for all acts committed through the hosted websites.[123]

The POS Guidelines further stipulate that computer networks for transmitting financial data over the internet must be demonstrated to meet the required standards specified for data confidentiality and integrity. The precise standards specified by the regulations are that all payment service providers comply with the Payment Card Industry Data Security Standards (PCIDSS), use as a minimum of 3DES encryption standard, and apply a minimum of two-factor authentication to verify users' accessing their systems and services.[124] The use of Public Key Infrastructure (PKI) is optional as the e-banking guidelines provide that banks

---

[122] See generally item 1.4.3 CBN E-banking Guidelines 2003.
[123] ibid item 1.4.8.
[124] See item 3.1 CBN POS Guidelines 2011.

may need to consider the use of PKI for authentication of users.[125] These requirements are further considered under respective headings below.

3.5.1.1 Industry Private Ordering System - Payment Card Industry Data Security Standards (PCIDSS)

PCIDSS is an established global standard for cardholder account protection across all parties in the payment chain. These include acquirers, third party processors and merchants.[126] The standards also apply to all entities that store, process or transmit cardholder data. It was developed in response to increasing incidence of cardholder account theft and is intended to help organisations proactively protect customer account data.[127]The standards are administered by the Payment Card Industry Security Standards Council (PCISSC), often simply referred to as the Council. Most Nigerian Banks are affiliated to global card schemes particularly VISA and MasterCard. They are therefore also obliged to comply with the PCIDSS by contractual agreements with relevant card schemes or networks.

PCIDSS standards are stated to follow common sense steps that mirror best security practices.[128] They are set to address vulnerabilities which may appear almost anywhere in the card processing ecosystem including points of sale (POS), personal computers, servers, web shopping applications, and unsecure transmission of cardholder data to service providers. They also cover vulnerabilities which may extend to systems operated by service providers and acquirers, including financial institutions.[129] The security controls are particularly vital for protecting Primary Account Number (PAN) and ensuring that service providers and payment card processors never store sensitive authentication data such as card verification value (CVV) or PINs after authorisation.[130] The PCIDSS focus primarily on internet facing card transactions, however, it applies to POS, mobile payments and telephone based order transactions as far as the provisions can be applied in such contexts.[131] The core framework of PCIDSS consists of twelve requirements organised under six functional goals as follows:

---

[125] Item 1.5.2 E-banking Guidelines (emphasis added).
[126] PCI payment Security standard Industry PCI Quick Reference Guide Understanding the Payment card Industry Data Security Standard Version 2.0 4.
[127] ibid.
[128] ibid version 2.0 5.
[129] ibid version 2.2 4.
[130] ibid version 2.0 11.
[131] ibid version 2.0.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel[132]

Table 3.3 -PCIDSS Goals and Requirements

The above table shows that PCIDSS requires a combination of physical, technical and operational measures to be implemented to protect cardholder data whether in storage or transmission.[133]

Much of the criticisms of the PCIDSS and how they translate in the Nigerian context are considered in greater details in chapter six. For the purposes of the analysis here, it is relevant only to emphasise that complying with the standards is mandated by the Central Bank of Nigeria (CBN). Item 3.1 of the POS Guidelines provides as follows:

> All industry stakeholders who process and/or store cardholder information shall ensure that their terminals, applications and processing systems comply with the minimum requirements of the following [PCIDSS] Standards and Best Practices … In addition, all terminals, applications and processing systems, should also comply with the

[132] See PCI DSS Requirements and Security Assessment Procedures Version 2.0 <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf> accessed 09/09/2013.
[133] ibid.

> standards specified by the various card schemes. Each vendor must provide valid certificates showing compliance with these standards, and must regularly review status of all its terminals to ensure they are still compliant as standards change. There will be a continuous review and recertification on compliance with these and other global industry standards from time to time.[134]

Another point worthy of mention is that in spite of this regulatory directive, statistics are disputed on the levels of compliance with the PCIDSS. As at 2011, only two of the potential target organisations were reported to be PCIDSS compliant. Contested reports also put the level of compliance at 2% in 2012 and up to 50% in 2013.[135]

3.5.1.2 Data Security – Authentication, Data Encryption, Digital Signature and Public Key Infrastructure (PKI)

The CBN guidelines also specify standards on authentication and encryption to be adopted by providers of electronic financial services. Generally, secured electronic communications are expected to meet four requirements. These are Privacy, Authentication, Integrity and Non-repudiation (PAIN).[136] Non-repudiation constitutes an assurance that neither of the parties can deny sending or receiving communication. In financial transaction terms, non-repudiation implies the finality of electronic payments. Integrity relates to the assurance that the data has not been altered. Privacy gives the assurance that no one apart from the intended parties has seen or read the contents of the message. Authentication provides proof of parties' identities and ensures that a message originated from the claimed source or entity.[137] Authentication is central to achieving privacy, integrity and non-repudiation in electronic transactions and is discussed further below.

(a) Authenticating Technologies

Authentication is the process of verifying or establishing identities. It differs from identification which is the process of associating one or more attributes with a person. Identification addresses the initial criteria for developing identity credentials, that is, who are you? Authentication asks the question, are you who you claim that you are? In other words, authentication addresses the question, how can you prove that you are the person registered or enrolled by the system? The OECD therefore defines authentication as the

---

[134] Item 3.1 CBN POS Guidelines.
[135] IT Security expert 2.
[136] See item 4.2 (d) (ii) CBN E-banking Guidelines.
[137] See generally OECD, 'OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication' (June 2007) <http://www.oecd.org/sti/interneteconomy/38921342.pdf> accessed 12/09/2013.

process which establishes 'the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system'. [138] Authentication is important for two reasons. One, it operates as a link between the claimed identity and the right and privileges flowing from that identity. Two, it ensures a sustained and continuous process of identification. For example, whereas identification is a one-off process, authentication is a repetitive process which occurs at every attempt to log into the providers system.[139] It is described as an essential component of any strategy to protect information systems and networking, as well as financial data, personal information and other information assets from unauthorised access or identity theft.[140] Financial authenticators are traditionally based on what the user knows such as PINS and passwords, or what he has, such as payment cards and tokens, or who he is which includes biometric characteristics such as fingerprints, iris scan and voice or facial recognition. Authentication processes may combine two or more identifiers to give a higher level of trust about the identity of a user. This is referred to as two factor authentication (2-FA) or multi-factor authentication. [141]

As already noted above, regulatory guidelines in Nigeria prescribe a minimum of two-factor authentication (or 2FA) for organisations verifying users' accessing payment information systems and services.[142] For example, the regulations on mobile money provide that 'all accounts activated by the consumer on the mobile application is linked to the mobile phone number [and] This mobile number shall be used as the second factor authentication for mobile transactions.'[143] Although, payment service providers argue that their organisations follow the CBN 2FA requirement,[144] research indicates that this is not the case. A survey shows for example that while ATM transactions conform to 2-FA, many online banking and payment services still use single factor authentication.[145] It was noted that while ATMs verify identity based on a combination of what the user knows (such as PINs) and what he has (such as the payment card), online banking systems continue to authenticate users by

---

[138] ibid 16.
[139] See Thomas J Smedinghoff, 'Introduction to Online Identity Management' 4 <http://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_-_Introduction_to_Identity_Management.pdf> accessed 21/07/2012.
[140]OECD, 'OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication' (n 137).
[141] For more comprehensive analysis of authentication protocols, see Xinyi Huang et al, 'A Generic Framework for Three-factor Authentication: Preserving Privacy in Distributed Systems' (2011) 22 (8) IEEE Transaction Parallel and Distributed Systems 1390.
[142] See item 3.1 CBN POS Guidelines.
[143] Item 4.1.9.7 CBN Mobile Payment Regulations 2009.
[144] This point was made by all payment service providers interviewed during the fieldwork.
[145] O.S Adeoye, 'Evaluating the Performance of Two-factor Authentication Solution in the Banking Sector' (2012) 9(4) International Journal of Computer Science Issues 457.

usernames or user-IDs and passwords which are all based on a single authentication protocol of what the user knows. If this position is correct, it can be argued that the 2FA minimum requirement is not applied uniformly across instruments, processes and channels of e-payments in Nigeria.[146] It is perhaps on account of this lack of uniformity that the CBN introduced the biometric verification number (BVN). The BVN exercise entails the registration of bank customers' biometric information which is to be used in combination with other authenticating technologies for banking and payment purposes.[147]

However, for the purpose of the arguments here, it is important to note that even where they are complied with, 2FA have limited use for e-commerce. For example, to satisfy the requirement of 2FA, some banks in Nigeria have also introduced token and SMS based one time passwords (OTPs). A OTP is a unique password valid for a login session or transaction.[148] Although, OTPs would satisfy 2FA because they involve the use of tokens or mobile devices (what the user has), they are only effective in bilateral relationships such as one existing between banks and customers. In other words, tokens are proprietary as they only support transactions with organisations that issue them.

Furthermore, notwithstanding how they are effected, a major challenge with authentication processes is their susceptibilities to criminal attacks. PINs, passwords, usernames and tokens can be stolen or compromised by hackers, phishers and malware. Recent research suggests that criminals can bypass authentication even in very sophisticated technologies such as those embedded in chip and PIN cards.[149] SMS based OTPs are particularly susceptible to criminal compromise including Man-in-the middle attacks discussed below.[150] It has also been argued that irrespective of layers of authentication processes, authenticators themselves have varying degrees of reliability. Those associated with biometric characteristics for example carry the risk of false performance.[151]

More crucially, authenticating technologies only function one way. This means that they authenticate one party such as the user to the provider but not vice-versa. In effect, while an

---

[146] ibid.
[147] See further notes in 5.1.3 CBN Bank Verification Number (BVN) p 139.
[148] Regulator 2.
[149] Mike Bond et al, 'Chip and PIN: Cloning EMV Cards with the Pre-play Attack' (2012) <http://arxiv.org/pdf/1209.2531v1.pdf> accessed 21/09/2013.
[150] See eg Colin Mulliner et al, 'SMS-based One Time Passwords: Attacks and Defence' (2014) <https://www.eecs.tu-berlin.de/fileadmin/f4/TechReports/2014/tr_2014-02.pdf> accessed 09/04/2015.
[151] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked Environment* (Wiley 2004).

organisation may be fairly certain that it is dealing with the genuine user, the user may have no means of ascertaining that he is dealing with the organisation he intends to deal with. This creates a gap in mutual authentication leading to lack of trust. To bridge the gap, banking regulations in Nigeria simply provide that banks must ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.[152] However, since technologically based security are often complicated and may be beyond the scope of the knowledge of individual users, secured information systems are often configured to execute mutual (self) authentication to the users.[153] In practice, a combination of data encryption, digital signatures and public key infrastructure (PKI) is used to achieve the needed mutual authentication. The following discussion on encryption, digital signature and public key infrastructure (PKI) demonstrates the technical processes of information security and the challenges of their implementation in Nigeria.

(b) Data Encryption

Encryption is the technological process used to convert plain or readable text into unreadable or cipher text.[154] The purpose of encrypting a message is to make it secret so that it is only intelligible to the intended recipient. Encryption is achieved by using a combination of mathematical formula called the cryptographic algorithm and a secret value referred to as the key. The mathematical formula or algorithm is used to encode or transform the message from plaintext to cipher text. However, the essence of encryption is not wholly to prevent a third party from obtaining the cipher text, it is also to prevent the deciphering of the message. This is where the key function becomes relevant. The key is a special knowledge or secret value used to encrypt the plaintext and to decrypt the cipher text. It is shared by the sender and recipient of the message, and messages can only be decrypted (converted from cipher text into plaintext) by a person or entity who knows the key. Therefore, even if an attacker intercepts the cipher text, he cannot access the plaintext unless he also knows the secret value or the key. A common example given to illustrate message encryption is Caesar's cipher. Caesar's algorithm substitutes each letter in the message with

---

[152] See item 4.1(f) CBN E-banking Guidelines.

[153] Web pages requiring SSL connections layered on HTTPS, an asymmetric algorithm supported by PKI is an example in this respect; see International Engineering Task Force (IETF), 'Network working Group, Request for Comments HTTPS over TLS' <http://tools.ietf.org/html/rfc2818> accessed 09/09/2013.

[154] Burton Rosenberg (ed), *Handbook of Financial Cryptography and Security* (Chapman & Hall 2010).

a letter which is 3 letters later in the alphabet and writes around to A from Z. Thus A becomes D and B becomes E and so on. The plaintext DOZEN would become cipher text CRCHQ. This formula is the algorithm and the number 3 is the key.[155] The algorithm here and the key appear quite basic, unsophisticated and insecure. They can be easily broken or guessed as there are fewer combinations to try, 26 alphabets in all.[156]

The strength of encryption therefore depends on the complexity of the algorithm and the length of the key. To be effective, a key must be sufficiently lengthy and must remain secret. A longer key generates longer combinations and makes it difficult to guess the key or to break it by brute force.[157] Cryptographic keys may be a private key or a public key. In private key encryption, also called a shared key, secret key or symmetric key, the same key is used to encrypt and decrypt the message. Examples of private key systems include the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) used to encrypt financial data. Consistent with this explanation, the prescribed standard for encrypting financial data in Nigeria is 3DES or TDES.[158]

It is to be noted however that even when key lengths are sufficiently strong, there are attendant problems of key management and distribution. This is particularly true of private key cryptosystem on the internet. Since private key systems use the same key to encrypt and decrypt the data, the key is susceptible to compromise because it could be stolen or intercepted in the process of exchange on the open networks of the internet.[159] Therefore, users need to find an additional secure channel for exchanging the key. To address the challenges of key distribution, public key encryption was developed. Public or asymmetric key encryption use different keys to encrypt and decrypt information. The public key system operates in pairs of private and public key. The public key is available to everyone and is used to encrypt information. The private key is required for decryption and kept secret by the owner of the keys. While the two keys are mathematically linked, they are designed in such a way to make it impossible to compute the private key from the public key. Relative

---

[155] See generally Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security: Private Communication in a Private World* (Prentice Hall 1995).
[156]ibid.
[157] Alfred Menezes, Paul Van Oorschot and Scott Vanstone, *Handbook of Applied Cryptograhy* (CRC Press 1997).
[158] See item 3.0 CBN POS Guidelines.
[159] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C* (John Wiley 1996).

to private key systems, public keys can be more secure because no key exchange is necessary and although the keys are linked, it is impossible to derive one from the other. [160]

(c) Digital signatures

As the above discussion demonstrates, the private key and public key cryptosystems are technically separate, however, in practice, a combination of different cryptosystems is used to achieve composite information security. For example, because of its speed, symmetric or private key is used to encrypt data. The private key is itself encrypted using the public key of an asymmetric key pair. A hash function is deployed to ensure the message has not been altered. In this case, only the private key holder can unlock the symmetric key and once the symmetric or shared key is retrieved, the recipient can now decrypt the original message. This produces a complex encryption process often difficult to break.

To illustrate, in order to create secure communication and ensure the authenticity of data between A and B, A first runs the message through an encryption algorithm to calculate the value of the message. This is the hash function which uses the number of words and the number of letters in a message to calculate the message value. The result produces a unique message called the message digest which has a value of say 500. A then encrypts the message digest with his (A's) private key (the key pair in public key system). This creates a digital footprint called a digital signature because only A has access to his own private key. A then generates a random key to encrypt the actual message. The random key is a symmetric or shared key for the particular transaction. It is also called a session key and needed because of the difficulties associated with key exchange and management in a symmetric key system discussed above. The session key is used once and then discarded. However, to send this particular session key to B securely, (the random key being a symmetric key is also the only key that can be used to decrypt the message and is still in A's possession), A encrypts the random key with B's public key. In this way, only B can decrypt the random key since he is the only one having his own private key. There is now multiple encryption; encrypted actual message, encrypted session key and encrypted digital fingerprint or signature.

In order to decrypt the message, B performs an inverse activity. B uses his private key to decrypt the random or session key. He then uses the recovered random key to decrypt the actual message. Although B now has the message and the key, he has no way of establishing

---

[160] Sanjay G. Kanade, Dijana Petrovska-Delacretaz and Bernadette Dorizzi, *Enhancing Information Security and Privacy by Combining Biometrics with Crypography* (Morgan and Claypool 2012).

that the message has not been altered. To check that the message has not been altered and is indeed sent by A, B uses A's public key to decrypt A's digital signature and recovers the message digest. B then runs the digest through the same algorithm or the hash function used to compute the digest. B generates a new message digest. However, B can only be sure that this is the same message sent by A if the new digest matches the original message digest precisely, in this case if the value is also 500.[161]

The process described above is the digital signature. In digital signature algorithms, the private key is used to sign a message and the public key is used to verify the signed signature. The process can be summarised simply as follows:

Creation

Message ← Hash function → message digest ← session key ←private key = digital signature

Verification

Digital signature = public key → session key →message digest ← hash function → message

Digital signatures are distinguished from simple electronic signatures by the technical process used to produce the signature.[162] However, as the mere execution of digital signatures does not also guarantee an entity's ownership of a public key, the reliability and effectiveness of digital signatures depend on verification operated under the public key infrastructure regime.

(d) Public Key Infrastructure (PKI)

PKI is needed because in spite of the complexity of the digital signature protocol described above, public key encryption is still susceptible to criminal compromise such as man-in-the middle (MITM) attacks. In a MITM attack, the attacker interjects himself between the two parties intending to communicate securely by impersonating himself as one to the other. The attacker does this by breaking the secure communication and inserting himself between the parties. He may then intercept and modify the communication to his own advantage. In the hypothetical scenario cited above for example, if A is a bank customer and B is the bank, a MITM attack can be perpetrated when A sends a message requesting B's public key and M

---

[161] See generally Kaufman, Perlman and Speciner, (n 155); see also Menezes, Van Oorschot and Vanstone, (n 157).

[162] See eg definitions of digital and electronic signatures in Regulation (EU) No 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market of 23rd July 2014, art 3 (hereinafter Regulation (EU) No 910/2014).

(the attacker) intercepts the message using malware or associated phishing or hacking tactics. Once he intercepts the message, M poses as B and sends his (M's) public key to A. A using this public key (which he believes to belong to B) sends an encrypted message to B e.g. to 'pay £1,000 into X's account'. M again intercepts the message to B and decrypts it with the corresponding private key because the published public key sent to A really belongs to M. M then modifies the message to read 'pay £10,000 into M's account'. M encrypts the message with B's public key (which he earlier intercepted) and sends the message to B. B, believing the message to be from A acts on the instruction and pays M.[163]

Since MITM attacks exploit real time processing, what the attacker does in lay terms is to intercept usernames, passwords, account numbers or payment card information for onward relay to the bank's server which cannot then distinguish the authentic user from the attacker because the information is encrypted. As noted earlier, encryption is not meant to protect the cipher-text as such but to prevent the retrieval of the plaintext from the cipher-text. Irrespective of the origin of the information therefore, encryption can be used to protect it. In effect, digital signatures based on public key systems do not also necessarily guarantee that encrypted information originated from an authorised or legitimate user. They do not solve the problem of how one can establish that one is communicating with the holder of the authentic or legitimate corresponding private key. Consequently, the problem associated with mutual authentication already noted above re-emerges. PKI is the additional technical infrastructure designed to support identity verification in digital signature systems.

PKI provides a way to validate the rightful owner of a public key. It is a framework for secure exchange of information based on public key cryptography and consists of the formal procedures used to verify keys by Certification Authorities or CAs. Although trust in a key system could be established bilaterally without the services of a trusted third party, public key cryptography usually implies that a trusted third party acts to certify the identity of an entity by means of an individual certificate.[164] According to the ITU specifications, the main components of the PKI are the digital certificates, the certification authorities, key management systems, and the laws, policies, software and standards regulating the security

---

[163] The above example is often given in different variants to explain man-in-the-middle attacks, see eg Chris Sanders, 'Understanding Man-in -the middle Attacks'<http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html>accessed 07/06/2015.

[164] Stephen Mason, *Electronic Signatures in Law* (3rd edn, CUP 2012) 92.

of information based on public key system.[165] The digital certificate strongly binds a public key to the name of the owner and is digitally signed by a trusted party called the Certification Authority.[166] The CA therefore attests the identity of an entity and verifies that the entity has the private key that corresponds to the public key associated with the certificate.[167] Accordingly, "certificate for electronic signatures" have been correctly defined as 'an electronic attestation which links electronic signatures validation data to a natural person and confirms at least the name or the pseudonym of that person'.[168]

Apart from issuing certificates, CAs also revoke certificates and are expected to create certificate revocation lists and maintain archives of status information about expired certificates.[169] CAs may themselves be certified by other CAs which creates a chain of trust until the user encounters the root Certification Authority which is a self-signed CA.[170] In addition to providing mutual authentication, PKI also generally meets the requirements of Privacy, Authentication Integrity and Non-repudiation (PAIN). For example, CAs provide mutual authentication by establishing the identity of an entity associated with a certificate. Digital signatures provide non-repudiation. Data encryption guarantees the privacy for communications. The hash function used in the encryption process ensures integrity of the data. Although PKI is not a mandatory requirement, the ITU recommends deployment of PKI for organisations providing secure services such as online banking and e-commerce services.[171] However, The Guidelines on Electronic Banking in Nigeria exempts mandatory use of PKI. The Guidelines provide, "…. Banks *may* [only] need to consider the use of Public Key Infrastructure (PKI) for authentication of users for e-banking services.[172]

The final requirement for the optimal functioning of the PKI is a legal framework. Digital signature laws provide this legal infrastructure. The laws provide the reference mechanism for establishing whether authentication protocols were duly executed and the evidential value to be attached to digital signatures. Remarkably, Nigeria does not also have a digital

---

[165]ITU-T Recommendations X.509 (11/2008) <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>accessed 14/12/2014.
[166] See eg ITU, 'Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications' (2003) <http://www.itu.int/itudoc/itu-t/85097.pdf>accessed 13/09/2013.
[167] ITU-T Recommendations X.509 (n 165).
[168] Regulation (EU) No 910/2014, art 3.
[169] ITU-T Recommendations X.509 (n 165).
[170] ibid.
[171] ibid.
[172] Item 1.5.2 CBN E-banking Guidelines (emphasis added).

signature law. Further implications of this deficiency for prevention of identity-related cybercrimes and for displacing existing fraud liability regime are discussed fully in chapter six.

It is therefore important to note that while data security measures are essential, they do not in themselves translate to composite protection in cybersecurity terms. Accordingly, the ITU defines cybersecurity in the following terms:

> …the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.[173]

The Internet Crime Complaint Centre (IC3) also depicts the process of combating internet crimes as an intricate puzzle comprising of pieces such as detection, compliant, mitigation, liaison, analysis, deterrence, investigation and prosecution and prevention.[174] The ITU definition and the IC3 observation suggests that the means for achieving cybersecurity include but are not limited to data security standards. It also suggests that its components include the protection of cyber structures and infrastructure, and the protection of users and user devices. Cybersecurity therefore implicates the consideration of laws, policies and actions for ensuring protection from cyber threats. These must include prevention and deterrence, identification and discovery, damage control and recovery as well as laws and policies that promote these measures. Therefore, whereas data security standards are often set by industry and applied at organisational levels and to different types of information, standards to protect personal information are set by laws such as data protection law.

Conclusion

As with cybercrimes generally, the scale and nature of fraud on e-payment systems are unknown. An examination of records, reports and organisational perspectives reveal that

---

[173] ITU-T, 'Rec. X. 1205 04/2008: Overview of Cybersecurity' (2008) 2 <https://www.itu.int/rec/T-REC-X.1205-200804-I> accessed 09/04/2015.
[174] Federal Bureau of Investigation Internet Crime Complaint Center, 'Internet Crime Report 2014' 6 <https://www.ic3.gov/media/annualreport/2014_IC3Report.pdf> accessed 01/06/2015.

there are no reliable estimates or assessment of cybercrimes that threaten e-payment systems. This is mostly due to the pervasive "culture of denial" in the Nigerian financial industry and policy inconsistency on definition and classification of the crime. However, in spite of lack of statistics, it is difficult to support assertions that cybercrimes are not pervasive on payment networks and systems. While payment service providers contend the threats of hacking to their own systems, they tend to argue that phishing is pervasively used to victimise users of e-payment services. The analyses however indicate that both service providers and users are susceptible to the cyber-threats, and in particular, service providers are likely to suffer large scale data breaches in consequence of hacking, phishing and the propagation of malware.

Therefore, as a basis for analysing the legal and regulatory frameworks in the remaining chapters of this thesis, this chapter established the cybercrime threats to e-payment systems. It also identified the relevant challenges posed by digital identities. The arguments in the chapter further demonstrate that at the level of policy and industry, industry's data security standards represents the main response to the threats posed to identity information.

Chapter Four

Criminal Law Responses to Identity-related Cybercrimes

Introduction

Cybercrimes may be broadly classified according to whether they are crimes using computers or crimes of computer misuse.[1] Crimes using the computer are typically traditional crimes such as fraud and theft. Computer misuse crimes include hacking which is a crime exclusive or specific to the technology. The underlying assumption behind the classification is that crimes using the computer could be dealt with by existing criminal legislation, while crimes exclusive to technology require new laws. This is largely contested by an alternative view which proposes that crimes using the computer, along with the real or exclusively-technology crimes, need to be regulated differently to real world crimes and both crimes require new laws.

This chapter examines these propositions in the context of the Nigerian criminal laws. It aims to determine whether and the extent to which the laws could be used to address specific cyber-threats such as hacking, phishing and identity theft and fraud. By comparative analysis of laws and judicial interpretations from the UK, the chapter will identify and discuss the problematic areas of the extant criminal laws and the proposed cybercrime law in Nigeria. Also, against the background of the empirical data the chapter will explore the societal, policy and judicial perceptions which may affect the effectiveness of criminal legislation in Nigeria.

The chapter therefore proceeds by examining the meaning and scope of cybercrimes. It follows with the analysis of the criminal law as they relate to relevant cyber-threats. The arguments focus in particular on the position of the Criminal Code Act and the proposed cybercrime law, the Cybercrime Bill 2014. The chapter concludes with the analysis of the administration and enforcement of the Cybercrime Bill.

[1] It is relevant to note that the use of the term 'computer' in relation to the crime is itself merely symbolic as the crimes can now be committed using other devices such as mobile phones or even non-devices such as the cloud infrastructure.

4.1 The Nigerian Law on Cybercrime

4.1.1 (Not) Defining Cybercrime

It was noted in chapter three that distinctions are made between computer crimes and cybercrimes depending on whether the crime is committed by a person internal or external to an organisation and whether it is committed on standalone or networked systems. For the purpose of the distinction, cybercrimes are limited to crimes committed using networked systems of the internet while computer crimes may be committed only on standalone computers. In spite of its apparent attempt at pragmatism, this distinction has become increasingly insignificant as a basis of definition. As the UNODC correctly asserts, 'In the hyper connected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime that does not involve electronic evidence linked with internet protocol (IP) connectivity.'[2] Brenner also argues that 'At some point, we can do away with cybercrime laws because most crimes will involve computers in some way, and all crimes will be cybercrime.'[3]

In effect, if computers will invariably become associated with most criminal activities, limited practical and legal advantages are derivable from any distinction. Following earlier analysis in chapter three, the notion that a crime is computer crime also carries the implication, at least at the level of organisations, of a wrongdoing internal to the organisation rather than one which is essentially criminal. It therefore presupposes and/or precludes the application of the criminal law to 'computer crimes' and suggests that perpetrators may be punished within the organisation rather than by the law. In essence the distinctions undermine the severity or seriousness of 'computer crimes' relative to cybercrimes. Generally, and correctly so, the UNODC considered distinctions between computer and cybercrimes as merely technical and legalistic if not impractical.[4]

Notably however, the UNODC offers two possible explanations for making the distinctions between cybercrimes and computer crimes particularly in developing countries like Nigeria. The first explanation is the possibility that cybercriminals in developing countries tend to focus more on domestic victims and possibly standalone computer systems. The second

---

[2] UNODC, 'Comprehensive Study on Cybercrime' (Draft February 2013) xvii. <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 12/12/2013.

[3] Susan W Brenner, 'Is There Such a Thing as "Virtual Crime" (2001) 4 Cal Crim Law Rev 1.

[4] UNODC, Draft Comprehensive study on Cybercrime (n 2) 6-8.

possible explanation is the inability of law enforcement in developing countries to identify transnational content in cybercrime due to capacity challenges.[5] In the Nigerian context, both explanations have some merit but the second explanation perhaps captures the problem more aptly. As arguments in chapter three suggest, cybercriminals in Nigeria victimised foreigners long before widespread victimisation of domestic users of computers and the internet.[6] Considering this context, it could be misleading to assume that the distinction between computer and cybercrime derives from the fact that cybercriminals focus on domestic victims or operate on standalone computers. Conversely, the relative inactivity of law enforcement and the judiciary in the area of cybercrime prompts the assumption that the second explanation offered by the UNODC is more applicable in Nigeria. In other words, capacity challenges may account for the artificial distinctions between these two concepts.[7]

Nevertheless, even if one takes the position that distinctions between computer and cybercrimes are unnecessary and ineffective, it is important to acknowledge that defining cybercrime remains a conceptual challenge. For example, while scholarly articles and commentaries in Nigeria appear to have engaged considerably with computer-related crimes, none has offered much help in the area of defining cybercrimes.[8] Criminal theorists have also argued against the notion that some crimes are essentially "cybercrimes". Grabosky contests the classification of a separate head of criminal law as cybercrime and argues that cyberspace is no more than a new environment for committing old crimes.[9] Brenner argues that unless they present new ways of imposing criminal liability, cybercrimes are no different to terrestrial or traditional crimes.[10] She opines that there is nothing like cybercrime as such and all crimes are just simply crimes.[11] Wall prompts an inquisition into both the rationale and the terminology used to describe the crime and argues that while the term has acquired considerable linguistic agency, it has no agreed meaning. He further posits whether we should be asking if there are actually such things as cybercrimes and if there is anything 'cyber' about the crimes.[12] Describing it as 'the transformation of criminal

---

[5] ibid 6.
[6] See notes in 3.1 Internet Fraud in Nigeria p 48 at 49.
[7] See notes below in 4.6.1 Lack of Computer Forensics Capacity in Law Enforcement.
[8] See eg Mohamed Chawki, 'Nigeria Tackles Advance Fee Fraud (2009) 1JILT 1; see also Taiwo Oriola, 'Advance Fee Fraud on the Internet: Nigerian Regulatory Response' (2005) 21(3) Computer Law and Security Review 237.
[9] Peter N Grabosky, 'Virtual Criminality: Old Wine New Bottles?' (2001) 10 Social & Legal Studies 243.
[10] Brenner, (n 3).
[11] ibid.
[12] David S Wall, Cybercrime *The Transformation of Crime in the Information Age* (Polity Press 2007) 9-10.

or harmful behaviour by networked technology',[13] Wall made the point that the term cybercrime is emotive rather than legal or scientific.[14] A similar point was made by Fafinski who noted that cybercrime is not a legal term of art.[15] Accordingly, correlate terms such as internet crime, computer crimes, and computer-related crimes, high-tech crime or information age crime have been used to describe cyber-related reprehensible conduct. Although each terminology may carry some variants in meaning, the literature suggests that while there are new and novel wrongful conducts which challenge traditional criminal law, cybercrime is no more than a useful metaphor to describe these perceived wrongful activities in the context of the peculiar environment of computing and networking.

In the particular context of the analysis here, defining cybercrime has limited use. Firstly, it is generally acknowledged that definitions are pointless if one considers the potentials of technology to generate deviant and wrongful behaviour and the difficulty (if not impossibility) of anticipating the scope of future wrongdoing which may be associated with computers or computing. Consistent with this position, the Council of Europe (CoE) Convention on Cybercrime, credited to be the first comprehensive attempt at addressing the problems of cybercrime, merely enumerated the specific activities which may constitute cybercrime rather than attempt to define the term.

Secondly, because there is considerable overlap between the general area of crime and cybercrime, cybercrimes are arguably still crimes. Crimes are generally acts or omissions forbidden by the criminal law and whatever their nature or scope, activities amounting to cybercrimes will not be criminal unless and until they are so defined by the criminal law. Accordingly, the Nigerian law prohibits the punishment of any person for an offence unless the offence is defined by law and the punishment thereof prescribed by the relevant law. Section 36(8) of the constitution provides, 'No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence,…' Similarly section 11 Criminal Code Act provides that 'A person shall not be punished for doing or omitting to do an act unless the act or omission constituted an offence under the law in force when it occurred.' This is in line with the rule of international law which applies the maxim *Nullum crimen, nulla poena sine lege* meaning nothing is recognised as a crime and no punishment appertains except as provided by law.[16] Therefore, even for the purpose of the analysis here, the term cybercrime is used quite presumptuously

[13] ibid.
[14] ibid.
[15] Stefan Fafinski, *Computer Misuse* (Willan Publishing 2009) 5.
[16] See eg Universal Declartion of Human rights 1948, art 11(2).

as extant criminal laws in Nigeria do not mention cybercrimes generally or expressly criminalise acts amounting to cybercrime.[17]

In order to aid the difficulties of definition, a helpful recourse is provided by the broad classifications of cybercrimes into crimes using computers or crimes of computer misuse. Crimes using the computer are typically traditional crimes such as fraud, and the threats they pose relate to the nature of the crime, and the scope, and reachability of the criminals. Computer misuse crimes, such as malware propagation are new crimes exclusive or specific to the technology. This distinction is helpful because it focuses on identifying areas where computer technology challenges the extant criminal laws. This may be in the sense of enabling relatively new forms of offending or in the sense that the technology merely aids or aggravates the commission of known or existing offences. The underlying assumption is often that crimes using the computer may be dealt with by extant or traditional criminal law while real cybercrimes require specific cybercrime legislation.

Therefore, a classification based approach avoids a prejudgement of the law because it forces an assessment of the extant criminal laws along with new or proposed responses to the crimes. In other words, examining the laws within the contexts of the classification forecloses conclusions that the criminal law in Nigeria does not deal with cybercrimes at all. For example, on the one hand, the empirical data suggests that a majority of stakeholders concede that cybercrime specific legislation is needed to combat emerging cyber threats.[18] On the other hand, the data suggests that extant criminal laws are being used or could be used to effectively combat cybercrimes. As Law enforcement 3 asserted, '... the problem is not that we don't have the laws, what we lack is the capacity' (that is, computer forensic skills). Another law enforcement agent cites examples of cases where existing criminal laws have been used to convict cybercriminals.[19] In the view of a policymaker however, 'so-called cybercrime convictions' are obtained through misuse of the plea bargain system as offenders are simply encouraged to plead to lesser or 'provable' traditional crimes to avoid indefinite prison detention. He asserts further that there are no data, facts, statistics, or cases to back up the claims of successful prosecution for cybercrimes.[20] The analysis below therefore starts by examining the responses of extant criminal laws to the respective threats

[17] See notes below in 4.2 Hacking under the Criminal Laws.
[18] 18 Respondents in all expressed this view. A similar position has been argued in the literature, see eg Oriola, (n 8).
[19] Law enforcement 1.
[20] Policy maker 2.

identified in chapter three. It then follows through with an assessment of how the proposed law on cybercrime aims to deal with the new threats.

4.2 Hacking under the Criminal Laws

Hacking is defined in chapter three as the use of technical means to access computer systems unlawfully or without authority. Hacking threatens e-payment systems because it is often the precursor to large scale breaches in proprietary networks. Although, it is considered a crime specific to technology, hacking has been variously compared to traditional crimes such as criminal trespass, burglary, or damage to property.[21] Accessing computer or network systems without authority is not expressly mentioned or criminalised under the Nigerian laws. However, a preliminary examination of the laws is necessary here to determine whether hackers could be prosecuted for trespass or related offences.

4.2.1 Hacking as Trespass

The Criminal Code Act criminalises housebreaking, burglary and like offences when committed with intent to commit a felony.[22] The Criminal Code provides as follows:

> A person who breaks any part, whether external or internal, *of a building*, or opens by unlocking, pulling, pushing, lifting, or any other means whatever, any door, window, shutter, cellar flap, or other thing, intended to close or cover an opening in a building, or an opening giving passage from one part of a building to another, is said to break the building.[23]

A person is deemed to have entered a property as soon as any part of his body or any part of any instrument used by him is within the building.[24] Based on the provisions of the Criminal Code, housebreaking or burglary must be committed with intent either to commit a felony or a further offence. Also from the provisions, the offences can only be committed with respect to homes, houses, buildings or similar property.[25] In context therefore, the provisions would not accommodate the notion of hacking which entails "breaking into" a computer system rather than a building, and where as noted below, the hacker need not have any ulterior motive of committing a further offence.

---

[21] See eg Law Commission, *Computer Misuse* (WP No 110 1998).
[22] s 410-417 Criminal Code Act.
[23] ibid s 410 (emphasis added).
[24] ibid.
[25] ibid ss 410-416.

4.2.2 Hacking as Damage to Property

Under the criminal code, any person who wilfully and unlawfully destroys or damages any property is guilty of an offence.[26] Property is defined as 'everything, animate or inanimate, capable of being the subject of ownership'.[27] Offences relating to property include destruction or attempt to destroy or cause injuries to any building or structure whatever, whether completed or not, any vessel, whether completed or not, any stack of cultivated vegetable produce, or of mineral or vegetable fuel, a mine, or the workings, fittings, or appliances of a mine.[28] Damage in the context of documents, writings or inscriptions includes acts which obliterate or render the document illegible in whole or in part.[29]

As the definition of property above clearly includes tangible property which is capable of being owned, it seems reasonable to conclude that the physical computer is property. To the extent therefore, that a hacker is deemed to have caused damage to the computer, a charge of damage to property can be sustained. It is however arguable whether the same interpretation could be applied to programs or information contained on the computer. For example, property is defined to include 'inanimate property'. While inanimate property may correctly be interpreted to include all forms of property including information, the law appears to have excluded such an interpretation. Sections 444 to 462 (of the Criminal Code) mentioned only buildings, mines, vessels, fittings and so on as the categories of property capable of being the subject of criminal damage. It would therefore seem reasonable to argue that the damage to property can only be committed in relation to 'tangible (inanimate) property' and not intangible property. If this is accepted as the correct interpretation of the law, one may also conclude that information or programs in the computer do not qualify as property. By extension, a hacker cannot be charged with damage if he copies, transfers, modifies or even erases personal information held on computer systems.

There is no case on this point in Nigeria but cases from the UK put the legal difficulties here in perspective. In *Cox v Riley*,[30] The defendant, a disgruntled employee had erased a computer programme which controlled a computerised saw belonging to his employers. He was charged with damaging the circuit card on the computerised saw. The prosecution argued that by removing the information stored upon the card, the defendant had damaged the card within the meaning of section 1(1) of the Criminal Damage Act (CDA) UK 1971. It

---

[26] ibid s 451.
[27] Ibid sch. Pt 1.
[28] Ibid ss 443-462.
[29] Ibid s 442.
[30] (1986) 83 Cr App R 54.

was argued on behalf of the defendant that since the programme or information did not exist in tangible form, it was not property which could be damaged within the meaning of the law.[31] The court rejected the argument and upheld the defendant's conviction on the grounds that erasing the program from the printed circuit card used to operate the saw also constituted damage to the printed circuit card (which is tangible property) within the meaning of the CDA. [32] Notably conviction was obtained in the case because damage to the information invariably also damaged the saw.

In R v Whiteley,[33] the appellant, a computer hacker had gained access into a computer network and altered data contained on discs in the system, thereby causing the computers to malfunction. On a charge for damage to property brought under section 1(1) of the CDA 1971, it was contended on behalf of the defendant that a distinction must be made between damage to the disc itself and damage to the intangible information held on it. It was argued further that impairment or alteration to the disc affects only the information but not the value or usefulness of the disc itself. Therefore, damage to software or to intangible information is not damage to the physical computer which is the tangible property. The court held that although the law requires that damage be to tangible property, it is not a requirement of the law that the damage itself be tangible.[34] The court in this case considered rather controversially, the nature of the damage itself rather than the character of the property. In other words, it was the damage which was intangible rather than the property. Nevertheless, the decision shows the unwillingness of the courts to apply the concept of 'damage to property' where mainly intangible property is involved. Invariably, to constitute damage under the law, the damage must also extend to or include some tangible property.

Subsequent amendment to the law addressed the problems caused by the above interpretations of the English laws. The law now provides that 'For the purpose of the Criminal damage Act 1971, a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.' [35] By this provision, destruction, modification or otherwise tampering with data is no longer tied to tangible property and recourse cannot be taken to the offence unless such modification invariably

---

[31] 'property' means 'property of a tangible nature, whether real or personal, including money…' see Criminal Damage Act (UK) 1971 s 10.
[32] *Cox v Riley* (1986) 83 Cr App R 54, 56.
[33] (1991) 93 Cr App R 25.
[34] ibid 27; see also *Morphitis v Salmon* (1990) Crim LR 48.
[35] Police Justice Act 2006, s 36 which amended s 3 Computer Misuse Act 1990.

leads to damage of the physical computer. According to Fafinski, the provision was intended to address the potential for overlapping liability with the criminal damage charges arising from cases such as *Cox v Riley* above. He argues correctly that the section thereby 'partitions electronic vandalism from physical vandalism'.[36]

Absent any such distinction under the Nigerian law, it must be taken that damage to property means damage to 'tangible inanimate property'. Information stored on a computer being inanimate but not tangible, cannot be "damaged" within the meaning of the criminal law. Moreover, as "damage" is implicit in the offence of damage to property, the basis of any logical extension further diminishes. For example, the concept of damage is inconsistent with the notion of hacking in the strict sense. By definition, hacking is unauthorised access to computer systems without reference to a resulting damage or the intent of the hacker. In other words, a hacker may access information, copy, and transfer or modify data without causing damage to the computer. In fact, as Nelson argues, 'it is far more common for the computer hacker to access a network without resulting in damage and to exit without ever been detected'.[37]

As the case of *Amadi v Federal Republic of Nigeria (FRN)*[38] also demonstrates, if an offender is at all convicted where his conduct or activities involve hacking, it would be because the prosecution looked to the results or effects of his action rather than the actual wrongful conduct which produced the result. The facts of Amadi's case are clearly that the defendant had accessed the systems of the Economic and Financial Crimes Commission (EFCC) without authority. He had cloned the website of the organisation and sent fraudulent mails purporting to be from the organisation. The defendant was however not charged with any offence having direct bearing on the underlying activity of hacking. It was argued that the prosecution obtained a conviction because it looked to the results (attempt to obtain money by false pretence) rather than the original wrongful activity (of hacking).[39] The effect of this reasoning is that defendant would not have been charged at all if he had simply hacked into the website and there was no evidence of his underlying motive to obtain money under false pretences.

---

[36] Fafinski, (n 15) 41.
[37] Brennan Nelson, 'Straining the Capacity of the Law: The Idea of Computer Crime in the Age of Computer Worm' (1991) 11 Computer LJ 299, 319.
[38] (2008) 12 SC (pt III) 55.
[39] Law enforcement 1.

Arguably, the most basic reason for taking this approach is to avoid the pitfall of charging the defendant with a non-existent offence. As mentioned earlier, a person cannot be punished for an offence which is unknown to law. In *R v Gold & Schifreen*,[40] the court in England applied the same reasoning to the specific case of computer related wrongdoing. The court quashed the conviction of the defendant on the grounds inter-alia that the act of accessing computer systems without authority did not constitute a criminal offence under English law.[41] According to Lord Brennan; 'The Appellants' conduct amounted in essence, …, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for legislature rather than the courts.'[42]

The case further highlights the difficulty of forcing computer crimes into existing criminal laws. Given the arguments above, the conclusion can be drawn that the position of the Nigeria law is that if a person breaks into the computer system of a financial or other institution or into a private account, such person incurs no criminal liability. A person can only be criminally liable if it can be shown that he has committed another or further offence such as damage to the physical computer or (attempted) theft or fraud. The following section examines the draft law on cybercrime to determine how it proposes to deal with hacking in Nigeria.

4.2.3 Hacking Offences under the Cybercrime Bill 2014[43]

A useful start point here is a brief highlight of the proposed law. The Cybercrime Bill 2014 was for an "Act to provide for the Prohibition, Prevention, Detection, Response, Investigation and Prosecution of Cybercrimes and Other Related Matters.' [44] It implements most of the provisions of the Council of Europe Convention on Cybercrime relating to offences, procedural powers and jurisdiction and international cooperation, and extradition and mutual assistance.[45] It is important to note that prior to the bill, several bills for cybercrime laws presented to the National Assembly were either not debated or not

---

[40] (1988) 1AC 1063.
[41] ibid 1071 para D and E.
[42] ibid.
[43] The bill was Cybercrime Bill 2013 at the time of collecting data for this research.
[44] Cybercrime Bill 2014 [SB 669].
[45] See Council of Europe ETS No 185 Convention on Cybercrime 2001; see also Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of acts of a Racist and Xenophobic Nature Committed through Computer Systems 2003.

subsequently passed into law.[46] The process (of presenting several bills) spanned over a period of 10 years.[47] The Cybercrime bill creates three categories of hacking offences. One, access to computer systems without authority, two, access in excess of authority and the three, unauthorised access with intention to access the contents of a computer.[48]

4.2.3.1 Access without Authority (Basic Hacking Offence)

Section 6(1) provides as follows:

> Any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000 or to both fine and imprisonment.

Under the foregoing provisions, intentionally accessing information systems without or in excess of authority is a Choate offence. Given the lacuna identified above relating to the difficulty of showing resulting damage in damage to property cases, this provision represents an attempt to bridge the gap in the criminal law. As the above provision shows, hacking will be an offence irrespective of whether consequences such as harm or damage results. Also, for the purpose of liability, a substantive offence need not be committed or even attempted; all that is required is that the offender accesses the computer system without or in excess of authority. Hence reference to the crime as 'basic hacking'.[49] However, construed literally, the provision is also inordinately wide and prone to latent ambiguities. For example, it does not carry the implication that the offender should intend to secure access to data or information or that he even knows that access is unauthorised.[50] Therefore, although the word *intentionally* supposedly underlines the *mens rea* of the offence, the effect of the provision is to create a strict liability.

---

[46] Although there could be more, 15 bills in all were located from manual search of legislative files at the National Assembly.
[47] Although the Cybercrime bill 2014 was reported to have been signed into law on 16 May 2015 just before the expiration of the tenure of the last government (government tenure expired on 29 May 2015), the version of the bill eventually passed into law was not available at the time of submitting this thesis.
[48] See s 6(1)-(2) Cybercrime Bill 2014.
[49] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 2.1.
[50] Compare Computer Misuse Act (CMA) (UK) 1990 s 1.

Based on the above observation, one may query the jurisprudential basis or even the moral culpability of the basic hacking offence. It has been argued for example that criminalisation (of hacking) is manifestly undesirable because it encroaches on certain fundamental freedoms. As Nelson argues;

> We might propose that the unauthorised access of a computer database is immoral because it violates the dignity of those who have labored and produced something of value over which they expect to exercise a certain amount of control. We might also argue that computer hacking is a moral affront to the right to privacy when a database contains personal information…However…According to the "alternative ethic," computer hacking is an expression of a fundamental human impulse.[51]

This "alternative ethic" also holds that criminalisation inhibits the hacker instinct essential for innovation. It further associates the hacker with the ideals of intellectualism and fanatism.[52] Infact, as Chandler suggests, the personal computer would never have existed without hackers.[53] Although, it is largely inaccurate, this controversial notion of the hacker persists in contemporary discourse and even the courts have tacitly endorsed it. In R v Bedworth,[54] the jury accepted the defence of computer addiction in acquitting the defendant. Also, in R v Cuthbert,[55] although the defendant was nonetheless convicted, the court considered him as deserving sympathy because of lack of malicious intent. The public support for 'pentagon hacker' Gary McKinnon in the UK and the eventual quashing of the order to extradite him to the US further suggests that the society differentiates between "ethical" and criminal hackers.[56]

Similar to the position above, the ethical and moral values at stake in computer hacking in Nigeria are also contestable. It was argued in chapter three that there is a tendency in Nigeria to undermine the hacker threats and see hackers as little more than activists (or

---

[51] Nelson, (n 37) 309.
[52] See Helen Nissenbaum, 'Hackers and the Ontology of Cyberspace' (2004) 6(2) New Media & Society 195,199-200.
[53] Amanda Chandler, 'The Changing Definition and Image of Hackers in Popular Discourse' (1996) 24 International Journal of the Sociology of Law 229.
[54] (unreported) 1991 in Yaman Akdeniz, 'Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Viruses' in Fafinski, (n 15) 54.
[55] (unreported) in Fafinski, (n 15) 60.
[56] See eg Graham Cluley, '71% Say Extradition Of UFO Hacker Gary McKinnon Is Wrong' (*Dark Reading*, 31/07/2009)<http://www.darkreading.com/71--say-extradition-of-ufo-hacker-gary-mckinnon-is-wrong/d/d-id/1131645?> accessed 02/08/2014.

hacktivists) who attack government owned websites in pursuit of radical social or political agendas.[57] Therefore, from the perspectives of organisations, there is no security urgency attached to the hacker threats. In addition, there appears to be perceptions that in terms of financial losses, cybercriminals pose relatively less serious threats. Law enforcement 1 notes for example that since most people have not been victims of cybercrimes, they tend to under-estimate the threats. Therefore, as he noted, '…they [the people or society] often imply that we [law enforcement] deal with the big criminals … [that is] the treasury looters… rather than petty [cyber] criminals.'[58]

These perceptions of cybercrimes and cybercriminals are also well documented in the literature. In their research into the social organisations of internet fraudsters in Nigeria, Tade and Aliyu found that mass youth unemployment and the corruption and impunity of public and political office holders were the explanations offered for the emergence of the yahoo-boys (internet fraudsters) sub-culture in Nigeria. The authors argue that the sustenance of the sub-culture itself is aided by society's propensity towards celebrating wealthy individuals irrespective of the source of wealth. Accordingly, since the system also fails to punish large scale fraud and corruption perpetrated by public officials, the society and the cybercriminals justify their crimes on grounds of necessity and survival and societal tolerance towards economic crimes generally.[59] To support the correctness of this position, music which extols the exploits of cyber-fraudsters has been promoted by popular media in Nigeria.[60]

It is remarkable that even among law enforcement and lawmakers, the view that hackers are relatively harmless also appears to be accepted. As noted by one law enforcement agent, since hacking and other cybercrimes only target financial data or money as against more serious crimes where victims could be assaulted or killed, they must be regarded as less

---

[57] See notes in 3.3.2.1 Hacking (Unauthorised/Illegal Access to computer Systems) p 56 particularly at 57.
[58] Law enforcement 1.
[59] Oludayo Tade and Ibrahim Aliyu, 'Social Organisation of Internet Fraud among University Undergraduates in Nigeria' (2011) 5(2) IJCC 860.
[60] See e.g. "I Go Chop Your Dollar" by Nkem Owoh and "Yahozee" by Olu Maintain, <http://news.bbc.co.uk/1/hi/entertainment/7670788.stm> accessed 15/03/2015.

serious.[61] He therefore described the offence as one perpetrated on the basis of 'your money or your money, and never your money or your life'.[62]

While this position undermines the fact that some online crimes can result in or be used to initiate real world assaults or injury, and therefore portrays a limited understanding of cybercrimes generally, this point is not considered further here.[63] The important inference in relation to the issue here is that views such as the above undermine the seriousness of hacking and related offences and may imply that law enforcement would rather dedicate time to the "more serious" offences than to comparatively "harmless crimes" such as hacking.

Finally, inferences drawn from records of legislative debates (on the cybercrime bill 2014) suggest that lawmakers also struggle to understand the basic hacking offence and the rationale behind its criminalisation. One lawmaker argued for example;

> '…the moment somebody has access to your computer, as long as it is not for something illegal or criminal and he is not taking your computer away permanently, you cannot say the person has committed an offence. If …I pick your computer system and I try to crosscheck a file, I do not think it is an offence. [64]

Consequent upon observations such as the above, lawmakers made proposals to amend the basic hacking offence in the cybercrime bill 2014. One of the proposed amendments states that, 'Any person who uses a computer to hack, obtain information or extract data or otherwise, create harm to the computer network has committed an offence.' [65] Another provides that, 'Any person who without authorisation intentionally accesses in whole or in part a computer system or network for fraudulent purposes commits an offence'.[66] Although, the amendments were not reflected in the bill eventually passed by the Nigerian Senate, the debate nevertheless indicates that the lawmakers miss the very mischief at which the law is

---

[61] Law enforcement 3.
[62] ibid; the idea here is that one can only lose money with cybercrime whereas people lose their lives to more serious crimes like armed robbery. This danger is often depicted in Nigeria by the statement ascribed to armed robbers who would ask victims at gunpoint for '*your money or your life*' meaning failure to surrender your money results inevitably in death. No one knows the exact origin of the phrase or whether armed robbers actually use it.
[63] See eg (n 105) below.
[64] Senate Hansard, vol 1 No 27 of Thursday 23rd October 2014, 9.
[65] ibid.
[66] ibid.

aimed. That is, that a person cannot hack or access a computer system simply because he wants to or because he can. Therefore, proposals that the hacker should have fraudulent or other intent to damage or otherwise make the computer unavailable would be irrelevant to the context of the offence.

The utilitarian and retributive theories of punishment provide some explanations which highlight the confusion surrounding the basic hacking offence. To illustrate, if one considers hacking from the perspectives of the retribution theory of punishment, it is possible to understand the jurisprudential basis of contesting a basic hacking offence. The theory proceeds on the principle that it is morally right to hate criminals and society extracts retaliation (for the crime) through the suffering of the offender based on a principle of equality or like for like.[67] Accordingly, punishment is justified only in response to a violation of the moral order. This implies that justice is inherent to the act of punishment and that punishment is consistent with and equal to the severity of the offence.[68] In context, to be fit for punishment, the hacker must cause some harm for which society seeks to extract desert. As noted above, unless hacking is followed by some form of secondary offending, the hacker may cause no actual harm or damage. Consequently, the basis upon which society seeks to vilify him may be unclear.

Conversely, when viewed from the utilitarian perspective of punishment, the hacking offence appears more defensible and pragmatic. The Utilitarian conceives punishment as having a goal beyond merely extracting retribution for a wrongful act. Utilitarians argue that punishment is itself evil and may only be administered if it promises to exclude some greater evil.[69] Therefore, punishment is justified only if it maximises utility in the sense that when balanced against the pains and cost, society finds punishment efficacious and profitable in preventing the mischief in question. According to Bilz and Darley, utilitarians assess what will happen as a result of different punishments, and weigh these outcomes against one another, and society may impose punishment only if the net result is that society will be better off.[70] To this end, punishment must be seen as having an instrumental value or

---

[67] Immanuel Kant 'Justice and Punishment' in Gertrude Ezorsky, *Philosophical Perspectives on Punishment* (Albany State University of New York Press 1972) 102-106.
[68] ibid.
[69] See Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation- A New Ed. Corrected by Author* (Volume 1 Oxford London 1823).
[70] Ken Worthley Bilz and John M Darley, 'What's Wrong with Harmless Theories of Punishment' (2004) 79 Chi-Kent L.Rev. 1215,1222.

socially beneficial consequences which utilitarianism conceives as deterrence, restriction and reformation of the offender.

Applied to hacking, the utilitarian approach shows that criminalisation is not necessarily aimed at extracting retributive justice for an inherent wrongfulness. It aims rather to achieve ends beneficial to society, which include protecting computers and networks and developing electronic transactions and commerce for the broader economic well-being of the society. This is consistent with the main justification often provided for criminalising hacking. That is the need to protect the confidentiality, integrity and availability of computer and information systems. Indeed, the underlying rationale for most basic hacking offences is that they serve as deterrent to the criminal and prevent secondary offending. According to the Law Commission for example, 'Basic hacking is proposed to be 'a simple means of deterring all hacker, whether fraudulent or malicious or not…' [71]

Nevertheless, while the utilitarian theory is useful in explaining and justifying an offence of basic hacking, its approach to punishment may give rise to concerns which are again relatable to the societal context in Nigeria. The utilitarian theory considers it immaterial that punishment fit the crime and may often impose punishments which appear excessive relative to the crime.[72] However, reasonably, and on grounds of principle and pragmatism, the seriousness of an offence is measured by the actual harm inflicted and punishment must reflect such seriousness.[73] The argument here is that if punishment is perceived as too severe, tensions may arise within the criminal justice system prompting a need for balance. To illustrate, section 6(1) of the cybercrime bill cited above, imposes punishment of 2 years imprisonment or fine of 5Million naira or both fine and imprisonment for the basic hacking offence. Against the background of the moral, social and even judicial perceptions of hacking noted above, one must consider the possible effects of this punishment on legitimising the offence.

To further illustrate, under the Nigerian Criminal Code, offences such as breaking and entry are not punishable unless a person breaks in with intent to commit felony.[74] Stealing which

---

[71] The Law Commission, *Computer Misuse* (WP No 110 1998) para 3.9.
[72] According to Bilz and Darley for example, 'if we ask, how much should we punish? He (the utilitarian) might answer "Exactly as much as is necessary to offset the bad effects of the crime", see Worthley and Darley, (n 70) 1223.
[73] See eg HLA Hart, *Postscript: Responsibility and Retribution' in Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford Clarendon 1968) 210, 235-36.
[74] See s 410 Criminal Code Act.

is a felony is punishable with three years' imprisonment.[75] Although, the Criminal Code is uncontrovertibly outdated,[76] these examples indicate that stiffer penalty for basic hacking may seem comparatively excessive if not outrightly illegitimate. In addition, precedents show that Nigerian courts tend to punish economic criminals comparatively less severely and they may impose small fines in lieu of imprisonment.[77] The Scottish Law Commission put the inherent difficulties here in perspective when it noted that 'The disadvantage (of a basic hacking offence) is that, on conviction of an offence …, a court might find it impossible to pass a more severe sentence…without reference to the actual or intended consequences.'[78]

Specific to the Nigerian context, it can be further argued that because hackers are often characterised as well-educated, young, technology-savvy individuals,[79] questions may arise on the desirability and utility of punishment. One may ask for example, whether it is desirable to expose such individuals to the full impact and severity of the penal system with its attendant stigmatisation and implications for recidivism.[80] The question is particularly relevant because with a fine of 5Million Naira[81] as an option to imprisonment, most convicted hackers are likely to end up in prison.

The above observations also find support in the fact that section 6(1) of the draft cybercrime law prescribes a mandatory minimum punishment which effectively bars judicial discretion on punishment. More precisely, since the bill provides that hacking attracts imprisonment for a term of *not less than two years or to a fine of not less than N5,000,000 or to both fine and imprisonment*,[82] the courts cannot exercise discretion either to reduce the length of imprisonment or the amount of the fine. Section 382 (1) of the Nigerian Criminal Procedure Code encapsulate the rule in this respect. It provides;

---

[75] ibid s 39.
[76] The Criminal Code is a colonial heritage enacted in July 1916.
[77] See eg Ihuoma Chiedozie, 'Nigerian Wonder: N27 Billion Pension Thief Gets N750,000 fine' *The Punch Newspaper* (Abuja, January 29 2013)<http://www.punchng.com/news/nigerian-wonder-n27bn-pension-thief-gets-n750000-fine/> accessed 04/08/2014.
[78] Scottish Law Commission, *Report on Computer Crime* (Scot Law Com No 106 1987) para 4.5-4.8.
[79] Law enforcement 1 and 3; see also Tade and Aliyu (n 59).
[80] See eg Isik Yusuf, 'Improving Prison Operations' (6th International Conference on Human Rights and Prison Reform Bangkok, Thailand 4th - 8th march, 2014) <http://www.internationalcure.org/Sixth-Presentations/Bangkok%20Yussuf.pdf >accessed 05/05/2014.
[81] This is approximately $25,000.
[82] S 6(1) Cybercrime Bill (emphasis added).

> Subject to the other provisions of [the] section, where a court has authority under any written law to impose imprisonment for any offence and has not specific authority to impose a fine for that offence, the court may, in its discretion, impose a fine in lieu of imprisonment.

However, under section 382(5), the provisions of section 382(1) shall not apply in any case where a written law provides a minimum period of imprisonment to be imposed for the commission of an offence. In effect, by prescribing a minimum mandatory sentence, the draft cybercrime law has eroded the courts' powers to exercise discretion on punishment. The approach to punishment taken under the Bill could therefore not only raise questions about the reformatory nature of the punishment and its overall utility to the society, it could also place additional pressure on the prison system which could ill-afford it.

It is important to conclude this section by stating that the argument here is not that hackers should not be punished. On the contrary, the argument is that further considerations be given to the issue of punishment particularly considering the nature and severity of the crime and the characteristics of likely offenders. Discretion on punishment by the courts for example could lead to more lenient punishment for "ethical" hackers who may then be rehabilitated or reformed. This position promotes the legitimacy of punishment and helps to avoid speculations of legislative overkill. As Nelson rightly observed, 'Where the law has lost the appearance of legitimacy, those who are called upon to behave or to refrain from behaving in a particular way are less likely to comply.'[83]

4.2.3.2 Unauthorised Access in Excess of Authority

As mentioned above, the draft law also creates the offence of accessing computer systems in excess of authority. Under section 6(1) 'Any person, …who without authorisation or *in excess of authorization*, intentionally accesses in whole or in part, a computer system or network, commits an offence…'.

The overall effect of the provision is to criminalise both accesses without or in excess of authority. However, access in excess of authority is particularly significant because of the relative greyness created by lack of corresponding provision in some computer crimes legislation. For example, section 1 of the CMA criminalises access without authority and is silent on access in excess of authority.[84] This has produced controversial and inconsistent

---

[83] Nelson, (n 37) 321.
[84] See CMA s 1.

judicial decisions. In *DPP v Bignell*[85], the Court of Appeal had upheld the argument that access in excess of authority is not a breach of sections 1 and 17(5) of the CMA. The court noted that based on its express provisions, the relevant sections of the CMA were directed at external hackers rather than authorised internal users who have authority to access their employers' systems.[86] The basis of the decision included a consideration of an arguably equivocal opinion of the Law Commission. The commission had drawn a distinction between outsiders' and insiders' access to computer systems. According to the Commission, insiders are people with legitimate access to a system who nevertheless exceed that (legitimate) access or use it for a wrongful purpose, while outsiders are what is typically thought of when talking of 'hackers'.[87]

However, in *R v Bow Street Metropolitan Stipendiary Magistrate and another, ex parte Government of the United States of America,* [88] the House of Lords relied on the same Law Commission report and held that the construction of sections 1 and 17 of the CMA was not to exclude misuse or 'hacking' by insiders or employees. As the court noted;

> Read as a whole, the report makes it clear that the term 'hacking' is used conveniently to refer to all forms of unauthorised access whether by insiders or outsiders and that the problem of misuse by insiders is as serious as that by outsiders.[89]

Therefore, by implying that the hacker is both a person who acts 'without authorization or in excess of authorization,' section 6(1) of the Cybercrime Bill avoids the tenuous distinctions which the English courts have had to make.

Furthermore, the provision arguably diminishes the needless and artificial distinctions between computer crime and cybercrime. As noted in chapter three, organisations tend to differentiate between insider and outsider fraud. The distinction in turn forms the basis of treating insider related computer frauds as computer crimes. However, the law now proposes to criminalise both accesses that breach code based restrictions as well as access based on employee misconduct. The invariable conclusion is that the insider who exceeds his authority is as much a criminal as the outsider who has no authority at all. Financial organisations must therefore report incidents of employee access to customers' personal

---

[85] [1998] 1 Cr App R 1.
[86] ibid 12-13.
[87] Law Commission, *Criminal Law-Computer Misuse* (n 49) para1.20.
[88] [1999] 4 All ER 1.
[89] ibid 10.

financial data if done in excess of authorisation as a breach of the criminal law. It is however to be noted that while the specificity and clarity of the provision (of section 6(1) is desirable in principle, its practical effects are contestable. For example, it is doubtful whether organisations will report 'internal hacking' because it has become a crime any more than if there is no criminal sanction. As was previously argued, there are reputational issues attached to security breaches whether they emanate from outsider or insider sources. As a result, organisations may be even less willing to press criminal charges against insiders and are more likely to use internal disciplinary procedures. Therefore, it can be argued that unless there is also a statutory requirement to report data breaches, the provision of section 6(1) regarding access in excess of authority may be largely ineffective.

Correspondingly, given the observations made with respect to access without authority above, it is arguable whether the approach of the courts, society or law enforcement will differ if a person merely acts in excess of his authority. In other words, the same arguments relating to relative harmlessness of the act and the severity of punishment may apply with equal force. In *R v Hardy*,[90] the English court took such an approach. The defendant, a police officer accessed police records and computers meant for police purposes for his personal purposes. He was charged with abuse of office and breach of duty of trust. In sentencing the defendant, the Judge referred to evidence of his good character and the difficulties he would face in prison, and thereby imposed a sentence of 28 weeks imprisonment, suspended for two years, and a period of community punishment. Although, the conviction was subsequently quashed on appeal and substituted with 9 months imprisonment, the case nevertheless demonstrates that courts may be predisposed to treating defendants charged with exceeding access with leniency. Consequently, offenders may be regarded as constituting even less of a threat than those who access with no authority at all.

4.2.3.3 Unauthorised Access with Intent to Obtain Computer Content

The proposed law appears to recognise that hacking is seldom an end in itself and thereby catalogues intended misuse which may follow accessing computers without or in excess of authority. Section 6(2) of the bill provides,

> Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, the punishment

[90] *Attorney General's Reference* (No 1 of 2007) 2007 All ER (D) 102 (Mar).

> shall be imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.[91]

On the face of it, the provision seems to complement section 6(1) by creating a 'hierarchical' level of offending.[92] Nevertheless, the provision is prone to fundamental interpretational challenges. It may be argued for example that the utility and effectiveness of the offence created by section 6(2) hinges on the correct construction of the word 'access'.[93] To see how, the bill provides that "access" in relation to an application or data means the following:

> …rendering that application or data, by whatever means, *in a form that would enable a person*, at the time when it is so rendered or subsequently, *to take account of that application or data including using the application or data or having its output from the computer system in which it is held in a displayed or printed Form*, or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not.[94]

Considering the aspects of the definition of access highlighted above, it can be argued that the basis on which a person could be charged for 'unauthorised access' under section 6(1) at all is if he has secured access to a program or data in the first place. For ease of reference, part of section 6(1) (already cited in full above) is reproduced as follows, 'Any person, who without authorization or in excess of authorization, intentionally *accesses* in whole or in part, a computer system or network…' The implication here is therefore that when the hacker commits the section 6(1) offence, he arguably has already committed the section 6(2) offence, or at least part it, (that is securing access to program or data). In other words, by merely accessing the system, without ulterior motive, the hacker has already taken account of or used an application or data and has consequently secured or obtained access to data or programs.

To further illustrate this point, an example given by the UK Law Commission is instructive. In the view of the Commission, there are three stages involved in logging into a computer system for access purposes. The first stage occurs when the computer user enters his identity code, his name, initials or password. In the second stage, the computer verifies the identity

---

[91] S 6(2) Cybercrime Bill 2014 (empahasis).
[92] See Law Commission, *Criminal Law-Computer Misuse* (n 49) para 3.11.
[93] See eg decision of the US courts in State v Allen 917, P.2d 848 (Kan 1996); see also State v Riley 846 P.2d 1365 (Wash 1993).
[94] S 48 Cybercrime Bill 2014.

of the user and if it recognises the user, grants access to the third stage where the user is allowed to use the facilities of the system.[95] According to the Law Commission, at stage three, the user unquestionably secures access to data or program held on the system and is therefore guilty of an offence. At stage two, he is guilty of an offence when he is verified by the computer because he intended thereby to obtain access to data or programs. The Commission also considers that the user is guilty of an offence at stage one because he already obtained information about data or program stored in the computer by finding out whether or not identification combination he presents is recognised as valid by a program held on the computer. In effect, securing access to a program includes running the program.[96] Following this reasoning, section 1 of the CMA defines unauthorised access in terms of causing the computer to perform any function with intent to secure access to any program or data.[97] Section (1) 2 CMA provides that where a person secures access to a program under section 1 of the law, he is nevertheless guilty of an offence although he does not intend to access;

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

This provision shows the broader breath of the CMA. For example, it is arguable that because it does not limit access to specific programs or information, the provision of section 1(2) above presupposes that by accessing a computer at all, a person already accesses any or some data or programs. By logical inference therefore, it is unnecessary to further specify that he access any particular program.

Against the background of this clarification, a person must be taken to have accessed data or programs once he logs into a system because 'logging-in' itself utilises a computer program. Therefore, since access to programs and data is a *sine qua non* to the basic hacking offence under section 6(1) of the proposed cybercrime law, unless the provision (of section 6(2) is framed in terms of securing access to a specific program, and not to *any program*, the section (or at least part of it) is repetitive and redundant. Consequently, it is open to the defendant charged with the sections 6(1) and (2) offences to argue that he intends only to commit the section 6(1) offence.

---

[95] Law Commission, *Criminal Law- Computer Misuse* (n 49) paras 3.16-3.18.
[96] ibid.
[97] CMA 1990 s 1.

The thrust of the foregoing argument is that by proposing to punish intent to secure access to a computer program or obtain data, section 6(2) seems to be a duplication of the section 6(1) offence. If this position is taken as correct, it may then be argued that charging a defendant with both offences has the potential of creating double jeopardy.[98] This may be fatal considering that the section 6(2) offence is more serious and attracts a stiffer penalty and is arguably the main mischief against which legislation is directed.

Even regarding the outstanding leg of section 6(2), that is, *intent to obtain commercial or confidential information*, the provision may be faulted on the grounds that what constitutes this category of information is not clear. The law fails to define this but defines content data as information stored on a computer memory.[99] The question this raises is whether 'commercial or confidential information (whatever it means) are the only categories of data which may be stored on the computer memory and thereby accessed by the hacker? Section 2 of the CMA also illustrates the point here. The section provides that a person is guilty if he commits an offence under section 1 CMA with intent inter-alia to commit any offence classified as further offences under the law. The CMA however omitted to define specific categories of further offences. According to the Law Commission, this approach was intended to create a 'preparatory offence' which covers a broad scope of 'further offences' or 'ulterior intent' offences. To provide the basis and justification for the offence, an example was cited of a hacker who breaks into the computer system of a banking organisation and succeeds in transferring funds. While he could be charged with theft immediately the fund transfer succeeds, the Commission expressed the view that it is unclear whether the hacker could be charged with attempted theft if he fails on account of being inhibited by the bank's computer security system. The Law Commission rationalised that the difficulty in such cases lay in the speed with which it is possible to transfer funds in computerised systems which makes it difficult to distinguish preparation from attempt for the purpose of allocating criminal liability. It was argued that when he defeats security checks such as gaining access by trying a large number of alternative passwords, the hacker, was merely at the preparatory stage for the substantive crime of theft. But because thereafter, transfer can be instantaneous, it becomes difficult to locate the point during the criminal transaction, at which he could be charged with attempted theft. The Commission opined that while attempt is not clearly discernible in cases such as this, the law should be such that

---

[98] The rule against double jeopardy is a cardinal principle of criminal law in Nigeria. In the strict sense, it means a person may not be tried twice for the same offence. However, it can also be pleaded in cases where multiple punishments may be imposed for the same offence, in which case the defence might apply to the court to strike out duplicate charges.
[99] See s 42 Cybercrime Bill 2014.

'a person, if he were detected trying to find the password, would at that stage have committed the offence of obtaining unauthorised access to a computer with intent to steal.'[100]

The basis of the preparatory offences was therefore to pre-empt secondary offending by exposing the hacker to prosecution at an early stage. However, because it is difficult to anticipate all categories of wrongdoing which a person may achieve by hacking into a system, the provision covers all types of secondary offending and not merely specific ones. As the Commission noted;

> We did not consider that it would be prudent or indeed possible to draw up a list of offences that might constitute such a 'further' offence, because it is not possible to draw up a finite list of the nefarious ends that a person might try to achieve by first securing unauthorised access to a computer. An indictment for the ulterior intent offence would contain particulars of the further offence allegedly intended.[101]

Correspondingly, drawing up a limited number of acts which may follow a hacking incident such as intent to obtain confidential data and so on, as done by section 6(2) of the Nigerian Cybercrime bill is limiting and undesirable. This is more so because intent is a notoriously difficult element to prove. It is trite law that a person is taken to intend the *actus reus* or forbidden act of a crime either in the ordinary, core sense of "intention" or in the sense that he recognised that the *actus reus* was a virtually certain consequence of his action.[102]

In spite of this clear direction, intention is a subjective concept and a particular *actus reus* could support multiple intentions. In essence, if a person hacks into a system, it may be difficult to establish what he intended to further achieve. In *R v Delamare*,[103] the intent of the defendant was to commit fraud on an account. In *DPP v Lennon*,[104] the defendant intended to, and did overwhelm the target website to cause a denial of service attack. In other words, while obtaining certain content may seem a natural or direct or foreseeable or virtually certain reason for hacking into a system, the overt act of hacking can also support a

---

[100] Law Commission, *Criminal Law- Computer Misuse* (n 49) para 3.52.
[101] ibid para 3.54.
[102] AP Simester et al, *Simester and Sullivan's Criminal Law Theory and Doctrine* (Hart Publising 2010) 127.
[103] [2003] EWCA Crim 424.
[104] [2006] EWHC 1201.

number of intent. This may include potentially more serious offences,[105] and those unrelated to computers.[106] The core of the argument here is that section 6(2) is limiting because it defines the specific results which must be intended by the hacker. The provision is therefore narrow and lacks neutrality, qualities which must be avoided even by technology focused or technology specific laws.[107]

In view of the above, a proposal may be made to expand the ambit of the proposed legislation. For example, although the position of the Nigerian law is that preparatory acts cannot attract criminal liability,[108] the provision of the Criminal Code clearly covers scenarios such as those discussed above. The Criminal Code provides;

> It is immaterial, except so far as regards punishment, whether the offender does all that is necessary on his part for completing the Commission of the offence, or whether the complete fulfilment of his intention is prevented by circumstances independent of his will, or whether he desists of his own motion from the further Prosecution of his intention. It is immaterial that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.[109]

Given this provision of the Code, even if the intention of the draftsman was to avoid the pitfall of so called 'preparatory offences', the section 6(2) offence can still be more broadly defined. Rather than defining the offence restrictively in terms of intent to obtain computer data, program or commercial or industrial secrets, the offence could be defined in terms of unauthorised access with intent to commit a felony, a misdemeanour, or to commit any offence defined by the cybercrime law or the general criminal law. For example, under the Code, breaking and entering is an offence if committed with intent to commit a felony. A felony in turn encompasses a wide scope of other offences and is punishable with a minimum of three years imprisonment. This is a more dynamic approach since the Criminal Code also accommodates the notion of general rather than specific intent. Section 24

---

[105] For example, the Law Commission cited the hypothetical case of hacking into a hospital computer which contains details of blood groups and rearranging the data with the intention that a patient should be seriously injured by being given the wrong blood; see Law Commission, *Criminal Law-Computer Misuse* (n 49) para 3.55.
[106] ibid para 3.57.
[107] See eg M Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (2nd edn ITU 2011).
[108] See *Dibia v State* (2012) l PERL 8564 (CA); see also *Yakubu Sanni v State* (1993) 4 NWLR (pt 285) 99, 199.
[109] s 4(2) Criminal Code Act.

provides that 'Unless the intention to cause a particular result is expressly declared to be an element of the offence constituted, in whole or part, by an act or omission, the result intended to be caused by an act or omission is immaterial'.[110] Therefore if D breaks into the computer systems of P bank, whether or not he intends to obtain personal data or program, he could be charged with the basic hacking offence and sundry offences. These may include intent to commit fraud, theft, blackmail or other computer-related or real world offences rather than the prosecution restricting itself to specific content offences.

4.3 Phishing- Fraudulent Representation and Computer-related Fraud

It is pertinent to state that the position and clarity of the law on phishing is important for three reasons. The first is that by the admission of the financial industry itself, phishing scams are the most pervasive method of compromising personal (financial) information in Nigeria.[111] The second reason relates to the pre-disposition of payment service providers to attribute security breaches to consumers and thus deny liability for fraudulent payments and fund transfers.[112] The third concerns assumptions that the laws which criminalise 419 scams also deal effectively with phishing.[113]

4.3.1 The Nigerian Criminal Law on Phishing, False Pretence and Electronic Payment Fraud

The laws in Nigeria did not mention or define phishing. However, it is generally an offence to obtain property by false pretence and with intent to defraud. Section 1(1) of the Advance Fee Fraud and Other Related Offences Act (hereinafter AFF Act) provides as follows:

> Notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud
>
> (a) obtains, from any other person, in Nigeria or in any other country for himself or any other person;
>
> (b) induces any other person, in Nigeria or in any other country, to deliver to any person; or

[110] ibid s 24.
[111] Nigeria Electronic Fraud Forum (NEFF) Annual Report 2012.
[112] See notes in 3.4.1 Account Takeover Fraud at p 70 at 71.
[113] See notes in (f) Spear Phishing p 66.

(c) obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act.[114]

A false pretence is defined as;

> … a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.'[115]

In *Federal Republic of Nigeria v Mike Amadi*,[116] the provisions cited above were applied to prosecute a cybercriminal. The defendant was charged with attempt to obtain money by false pretences contrary to sections 5(1), 8(b) and 1(3) of the Advanced Fee Fraud and Other Related Offences Act (AFF Act). He was also charged with forgery contrary to section 468 of the Criminal Code Law. On appeal to the Supreme Court, the defendant was convicted on the counts of attempt to obtain money by false pretence and forgery and acquitted on the count of uttering forged document.[117]

The significant aspect of the case is that while it is cited as the major breakthrough in cybercrime conviction in Nigeria,[118] the claim can generally be faulted. For example, although the facts indicate that the defendant hacked into and cloned the website of the EFCC, the defendant was not charged with any offence(s) bordering on (mis)using computer or using the internet as a medium for the attempted crime. The references to the facts of computer use in the case are as follows:

> PW2…Based on his investigations informed me that the Internet Service Provider for the cloned EFCC website is Multi-Links…requesting them to provide the details of the subscriber to that number…based on the information,…the accused person was arrested at his residence, we met the accused person using his computer. We arrested him and recovered the system.

---

[114] Similar provisions are contained in s 419 Criminal Code Act.
[115] s 20 AFF Act; see similar provisions in s 418 Criminal Code Act.
[116] (2006) 1 Economic Crimes Law Report 15.
[117] See *Mike Amadi v Federal Republic of Nigeria* (2008) 12 SC (pt III) 55.
[118] Law enforcement 1.

> We recovered the receipts of the purchase of the Internet number….. the 1st E-mail that complained against the fake E-mails that were purportedly sent…[119]

By refraining from bringing any charges for wrongful use of the computer or the internet, the prosecution in Amadi's case arguably avoided what has been described as the procrustean attempt to force the facts a case into the language of an Act not designed to fit them.[120] The only aspect of the case relied on to qualify it as a cybercrime conviction relates to the admission of e-mails as evidence. However, this only further diminishes the basis of classifying the case as one of cybercrime because while the admission of e-mail as evidence is relevant, it is hardly significant. The AFF itself defines 'document' to include a document transmitted through fax or telex machine or any other electronic or electrical device, a telegram and a computer printout.[121] By definition therefore, email evidence is already admissible under the AFF Act. As the Nigerian Supreme Court confirmed, the defendant was convicted because he had made false pretences to an *identified person* by means of *letters* (e-mails) containing the false pretence. [122]

More significantly, since the evidence in Amadi's case was obtained largely through an agent provocateur, it can be argued that evidence was carefully and deliberately collected. One may therefore ask whether the court would have reached a similar conclusion if it had been faced with a classic case of fraudulent transfer or attempt to transfer funds electronically. This is in particular where the false pretence was not made to any *identified person* but to a machine.

To make the argument clearer, reference may be made to judicial decisions in the pre-Fraud Act era in the UK. Although, UK law defined sundry fraud offences before the Fraud Act,[123] the courts still faced difficulties when interpreting the concepts of obtaining property by deception or false pretence in relation to computerised systems. For example, the relevant sections of the Theft Act 1968 provides that 'A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment…'[124] "Deception" means

---

[119] *Amadi v Federal Republic of Nigeria*, (n 117) 74 paras 5-15, 35.
[120] See *R v Gold & Schifreen* (1988) 1AC 1063, 1073 para B.
[121] s 20 Advance Fee Fraud Act.
[122] *Amadi v Federal Republic of Nigeria*, (n 117) para 35.
[123] The law created eight deception offences which make it criminal for a person dishonestly to bring about a number of specified consequences by deception. See Theft Act 1968 ss 15-16 (repealed by Fraud Act 2006).
[124] Theft Act 1968 s 15(1) (repealed).

any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person.' [125] According to the Law Commission, the concept of deception was introduced by the Theft Act 1968 in place of the older concept of 'false pretence' which was broadly synonymous with fraudulent misrepresentation. The aim was to 'move the focus away from the defendant's conduct to the deceived person's mistaken belief.[126] According to the Commission, 'the word "deception" seems to us… to have the advantage of directing attention to the effect that the offender deliberately produced on the mind of the person deceived, whereas "false pretence" makes one think of what exactly the offender did in order to deceive.'[127]

The authorities suggest therefore that the distinguishing factor is that false pretence may be made by one person without necessarily deceiving the person to whom the false pretence was made, whereas deception requires that the deceived party be actively misled. As the Commission observed;

> [To] say that the defendant has deceived another person implies that the other person believed in the truth of the defendant's false representation. Sometimes however, a person believed in the truth of the defendant's false representation without actively considering whether or not it is true. Arguably such a person has not been truly deceived.[128]

However, as the Law Commission further noted, although the change in nomenclature, that is from false pretence to deception, was not expected to have significant practical effects, the outcome of a number of cases suggest otherwise. [129] In R v Lambie, [130] the Court of appeal applied the distinction to quash the conviction of the appellant for obtaining pecuniary advantage by deception under section 16(1) of the Theft Act 1968. The Court conceded that the facts had established that the appellant had made a false pretence or false representation in that she had made a representation that she was authorised by the bank to use her credit card, when in fact she had exceeded her credit limit. The Court however further reasoned that to sustain a conviction under s 16(1) of the Act, it was necessary to show that that the person to whom the representation was made had acted or relied on that

---

[125] ibid s 15(4).
[126] Law Commission, *Fraud* (Law Com No 276 Cm 5560 2002) para 3.26.
[127] ibid.
[128] ibid para 3.29.
[129] ibid para 3.27.
[130] [1981] 1 All ER 332.

representation. Since the evidence in the case had shown that the shop assistant to whom the false pretence was addressed was not thereby deceived, the court allowed the appeal and quashed the conviction.[131] This case is particularly relevant in the context of payment cards. For example it suggests that in spite of the fact that a card is stolen or used without authority, the 'fraudster' may be acquitted because although he had made a false pretence, the merchant was not consequently deceived.[132]

R v Preddy[133] further highlights the complications introduced by the concept of deception in fund transfer cases. The facts are briefly that the defendants had by means of applications containing false statements obtained or attempted to obtain mortgage advances from building societies or other lending institutions. They obtained advances which were effected through telegraphic or electronic transfer and which involved the debiting of the lenders account and the corresponding crediting of the accounts of the appellant or his solicitor. The court rejected the contention that the credit on the appellants account represented 'property belonging to another' which was obtained by false pretence. As the court reasoned, the debiting of a bank account and the corresponding crediting of another's bank account brought about by dishonest misrepresentation does not amount to the obtaining of property within the meaning of section 15 of the Thefts Act 1968.[134] Accordingly, the credit being a chose in action never belonged to lenders and came into existence belonging to the payee/appellants. This decision means in effect that an individual who obtains any form of payment or any form of banking transfer by deception cannot be prosecuted because he has not thereby obtained property belonging to anyone.[135]

The difficulty created by Preddy was addressed by amending the Theft Act. A new section 15A made it an offence to dishonestly obtain a money transfer by deception. However, as subsequent cases show, this again did not wholly cure the defect in the law. In particular, problems persisted because courts continue to hold that a person rather than a computer must be deceived in such contexts.[136] Therefore, with regards to the question whether a computer can be deceived, the authorities were at first conflicting. The court in *R V Charles*

---

131 *R v Lambie* [1981] 1 All ER 332, 334 - 340.
132 See eg *R v Charles* (1977) AC 177.
133 [1996] AC 815.
134 ibid 833-835.
135 See eg Law Commission, *Offences of Dishonesty: Money Transfers* (Item 11 of the Sixth Programme of Law Reform 1996) para 1.7.
136 See eg *Holmes v Governor of Brixton Prison* (2004) EWCH 2020 (Admin); see also Rhys Bollen, 'Continuing Confusion over What a Payment Is' (2005) Cambridge Student Law Review 31.

noted orbiter that deception is the misleading of a particular person or thing.[137] However, in *R v Gold & Schifreen*, the court considered, again orbiter, that a machine such as a computer cannot be deceived. According to the court;

> The prosecution had to prove that the [respondents] intended that someone should accept as genuine the false instrument they had made. The suggestion here is that it was a machine...which the [respondents] intended to induce to respond to the false instrument...If that is a correct analysis, the prosecution case is reduced to an absurdity...[138]

To address the problems highlighted above, the Fraud Act repealed the problematic provisions of the Theft Act.[139] It criminalised express or implied representation, including representations made to machines or devises whether or not they are acted upon by any (intended) human recipients.[140] The Act provides, 'For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)'.[141] It has been argued, quite correctly, that these provisions mean that there is no limitation to the ways in which a representation can be made and include representation posted on a website or sent through an e-mail.[142] The correct interpretation is therefore that the provision covers all forms of phishing activity whether directed at a person or a computer.[143]

As noted above, the Nigerian law defines and applies the concept of false pretence. However, having considered the subsequent legal problems raised by the concept of deception under the Theft Act and how the Fraud Act resolved them, the relevant point for consideration is the position reflected in the Nigerian law. In other words, does the concept of false pretence in Nigeria reflect the position of the English law under the repealed provisions of the theft Act or does it embrace, without need for reform, the interpretation of the Fraud Act to effectively deal with phishing?

---

137 *R v Charles* (n 132) 178.
138 *R v Gold & Schifreen* (n 120) 622-623 (Lord Lane CJ).
139 See Theft Act 1968 ss15, 15A, 15B and 16.
140 Fraud Act 2006 s 2(4), (5).
141 ibid s 2 (5).
142 See Anne Savirimuthu and Joseph Savirimuthu, 'Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective' (2007) 4(4) Scripted 441-444.
143 ibid.

If one accepts the distinctions made above between false pretence and deception, it is possible to argue that since deception is not an element of the offence under Nigerian law, then the question of whether a computer is deceived in phishing scams or fraudulent transfer of funds can become irrelevant. As the definition above shows, the AFF Act simply defines false pretence without requiring that it be made to any person or thing.[144] As also noted above, this was indeed the intended effect of a false pretence as distinguished from deception.[145] However, even if this interpretation is correct, on judicial authority, there is a lacuna here. *Amadi v FRN* gives some indications of the reasoning of the court and what would perhaps have been its response if there had been a suggestion that false pretence was made to a machine or a computer. According to the court;

> …counsel for the appellant has submitted that before a conviction can be sustained for the offence of attempt to obtain money by false pretences…there must be a fraudulent pretence contained in a document from an accused to *another clearly identified person*. It must be clear that the document emanated from the accused and it was meant to be received and was infact received by the victim if such pretence is contained in a letter or other documents.[146]

The court appeared to accept that this is the correct position of the law when it held that the prosecution had discharged the burden (of proving that fraudulent pretence contained in a document from an accused was made to *another clearly identified person).* In other words, a false pretence is required to be directed at a person.[147] To further support this finding, the court restated the provisions of section 5 of the AFF Act to the effect that, '…it shall be sufficient in a charge of an attempt to commit an offence under this Act to prove that the letter or other document was received by *the person* to whom the false pretence was directed.'[148]

Considering this further requirement, not only is it essential that the false pretence be directed at a *clearly identified person* but it must also be received by *the person* to whom the pretence was made. These requirements are arguably difficult to meet in the context of fraudulent fund transfers over the internet. By nature, phishing mails need not be directed to

---

[144] See s 1 AFF Act.
[145] See *R v Lambie* (n 131).
[146] *Mike Amadi v Federal Republic of Nigeria* (n 117) 74 paras 10-15 (emphasis added).
[147] See *Uzoka v Federal Republic of Nigeria* (2009) LPELR -4950 (CA) 8-29 (emphasis added).
[148] s 5(1) AFF Fraud Act 2006.

any particular person. They may originate as spam aimed at inducing prospective victims to click on links to spoofed sites. Also, malicious software can be used to trick out personal (financial) information without the knowledge of the victim. In either case, the fraudulently obtained information could be fed into the computer system of a banking organisation and fund transfers may be achieved by *tricking* the system independently of any human intervention.

It is notable that in addition to directing the false pretence to a clearly identified person, the definition of false pretence under section 1 subsection 1 of the AFF (already cited above) also requires that there be intent to defraud. Although the law did not also define what constitutes intent to defraud, the courts have established that this carries an element of intent to cause economic loss. In *Awobokun v The State*,[149] the Nigerian Supreme Court quoted with approval the definition of intent to defraud given in *Welham v DPP* as follows; ….'with intent to defraud' means 'with intent to practice fraud' on *someone or other*. It need not be anyone in particular. Someone in general will suffice. If anyone may be prejudiced in any way by the fraud, that is enough….'[150] Based on judicial authority, intent to defraud must also manifest in relation to persons and not machines. By logical extension therefore, if a person cannot deceive a machine or computer, he cannot also defraud a computer.

The analysis above shows that in spite of the fact that the AFF Act prefers the term 'false pretence', logical application of the law means that the Nigerian courts will follow the interpretations of the English Courts under the repealed provisions of the theft Act. False pretence therefore has the same implications and effect as deception.

4.3.2 Computer Fraud under the Cybercrime Bill

The foregoing analyses demonstrates that the problem is not so much that it is completely impossible to secure convictions in cases where computers constitute an aspect or a medium of fraud, but that the cases do not reflect the true nature or character of the crime. Accordingly, one would expect the proposed law on cybercrime to address the issues less technically and more pragmatically. However, a perusal of the provisions shows that this is not the case. Section 12 of the bill creates 'computer related fraud'. It provides;

> (1) Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or

---

[149] (1976) 4 SC 2.
[150] *Welham v DPP* (1961) AC 103, 133 (emphasis added).

suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits for himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.

(2) Any person who with intent to defraud sends electronic *message to a recipient*, where such electronic message materially misrepresents any fact or set of facts upon which reliance *the recipient or another person* is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.[151]

First, it is unclear why the phrase '…without legal authority or in excess of authority' was included in the definition of computer related fraud in section 12(1) above. For example, one may be constrained in thinking up cases where causing loss of property to another by altering, erasing, inputting or suppressing data could be done with legal authority or in excess of authority, except perhaps for the purposes of investigation by law enforcement. The section would perhaps be clearer if the offence is defined with reference to mental elements such as knowingly or intentionally or recklessly causing loss of property to another. Exceptions may then be limited to use by law enforcement or protection of national security if this was intended.

Second, by stating in section 12(2) that reliance must be placed by the *recipient or another* person on the electronic message, the bill merely restates the position of the extant criminal law. In other words, the fraudulent electronic messages must be sent to a *recipient* who must have suffered damage or loss by reliance on it. On account of the peculiarities of phishing mails and the dangers they pose to information systems, one would have expected the bill to criminalise the very act of sending fraudulent/phishing mails. Like the AFF Act therefore, the implications of the provision is that the law will always look to find results such as the commission of actual fraud.

To illustrate this point, if a person sends a mail purporting to be from a bank requesting for the account details of the recipient or asking that money be transferred by the recipient to him or any other person, the effect of the provision (of section 12(2) will be that no offence has been committed unless and until the recipient responds to the bait and losses money in

[151] s 12 Cybercrime Bill 2014 (emphasis added).

consequence. More fundamentally, unlike the express provisions of the Fraud Act,[152] the provisions imply that the fraudulent electronic messages must be addressed to a human *recipient* not a machine. The difficulties inherent in this approach have been discussed above and need not be repeated here. However, it is necessary to note that separation of digital identity of things from that of humans would facilitate legal recognition that things like computers can also be deceived. As will be argued later in chapter five, such distinctions would also considerably abridge the needlessly infinite category of personal information. For the purpose of the arguments here, it is important to note that the inference is that the new provisions in the cybercrime bill are not sufficiently precise to cause a shift in the approach the courts are likely to take to phishing scams and computer fraud.

4.4 Spamming, Malware Distribution and Modification and Damage of Computer Programs

Spamming and malware distribution are examples of exclusively technology crimes because they cannot be committed independently of computers and networks systems. There are therefore understandably no provisions in existing criminal legislation dealing with this area. Under section 8 of the Cybercrime Bill, any direct or indirect act without authority and with intent to cause unauthorised modification to any data held in a computer or network is an offence. Also, any damage, deterioration, alteration, or suppression of data including transfer of data without authority is an offence. Both offences are punishable with 3years imprisonment or 7million Naira fine or both.[153] For the purposes of the section, a modification is defined as follows:

> A modification of any data held in any computer system or network takes place where, by the operation of any function of the computer, computer system or network concerned any-
>
> (i) program or data held in it is altered or erased;
>
> (ii) program or data is added to or removed from any program or data held in it; or

[152] See Fraud Act 2006 s 2 (5).
[153] s 8(1), (2) Cybercrime Bill 2014.

(iii) act occurs which impairs the normal operation of any computer, computer system or network concerned.[154]

Damage in the context of the law means impairment to the integrity or availability of data program, system or information. [155] Section 9 of the Bill creates the offence of system interference. This consists of activities similar to section 8 above or any other form of interference in the computer system, which prevents the computer system or any part of the system, from functioning in accordance with its intended purpose. Such interfere attracts imprisonment of not less than 2years or 5million naira fine or both.[156]

While it is not specifically stated, the provisions above may be extended to modifications, damage or interference caused by spamming, and denial of service attacks. Section 9 in particular may apply to spamming to the extent that spam mails interfere with computer systems without causing modifications or any of the consequences prescribed by section 8. Also, if spam disguises malicious software, an offence would be committed. Section 10(5) provides that using automated means or device or computer program or software to retrieve, collect, or store passwords, access codes or other means of gaining access into a program, data or database held in a computer system is an offence. The offence attracts imprisonment of not less than five years or a fine not less than 10million naira or both.[157]

As the above provisions show, bare spamming is not an offence unless it also interferes with the functioning of the system or is disguised as malware to collect or harvest identity information. On the one hand, this may be a good approach considering that spamming may raise arguments similar to those considered under hacking above. In other words, one may need to justify the offence by evaluating its harmfulness. [158] This is more so because spam may originate not only from criminals but also legitimate businesses and to that extent may constitute abusive market practices rather than a crime. On the other hand, because fraudulent or phishing mails often originate as spam, arguments justifying the criminalisation of phishing made above apply with equal force. One way to resolve the conflict is to regulate 'legitimate spamming' through data protection laws which define organisations obligations with respect to the processing of personal data.

---

[154] ibid s 8(3).
[155] ibid s 42.
[156] ibid s 9.
[157] ibid s 10(5).
[158] see previous notes in 4.2.3.1 Access without Authority (Basic Hacking Offence) p 97 at 101.

Finally to address the threat posed by malware, the cybercrime bill criminalises the unlawful development, production, possession, sale, distribution, or otherwise propagating malware, exploit software and other tools designed to overcome the security of computer systems.[159] Disclosing passwords, access codes or other means of gaining access to a program or data in a computer or network knowingly or without authority are also offences under the bill.[160] Apart from their specific relevance in the context of controlling fraud on e-payment platforms, these latter provisions are also helpful in undermining the distinctions between computer and cybercrimes. While not expressly directed at insiders for example, section 10(3) captures the activities of insiders who may abuse their positions to access password, access codes and similar identifying information. In effect, the provisions bring even such insider activities within the ambit of cybercrimes rather than restricting them to computer crimes.

4.5 Identity Theft and Identity Fraud under the Criminal Code Act and the Cybercrime Bill

Putting the problem of identity theft in e-payment systems in perspective, Schreft noted as follows:

> Identity theft is profitable precisely because today's economy is information dependent. Information flows where cash once changed hands at the point of sale. False information is the equivalent of counterfeit currency or stolen and forged checks. It is no wonder that identity theft is a problem of the modern payment system.[161]

Chapter three discussed the notion of identity and noted that hacking, phishing and malware propagation are used by criminals to target identity or personal information. It was argued further in the chapter that the successful prosecution of the activities often result in identity theft and identity fraud. However, before considering the position of the criminal law on identity crimes, it is necessary to highlight the conceptual differences between identity theft and identity fraud as they tend to be used interchangeably or defined one in lieu of the other. As an example, the OECD defines identity theft as occurring 'when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other

---

[159] See s 10(1), (5) Cybercrime Bill 2014.
[160] ibid s 10(3).
[161] Stacey L. Schreft, 'Risks of Identity theft: Can the Market Protect the Payment System? (2007) Federal Reserve Bank of Kansas City Economic Review Fourth Quarterly 5, 21.

crimes'.[162] This definition is not particularly apt as it combines the elements of two separate conducts. One is the unlawful obtaining of personal information and the other is the subsequent misuse of that information. The first conduct which may be described as the 'true identity theft',[163] includes the exposure of another's personal information without explicit permission[164] or 'any impersonation of a specific individual.'[165] The second conduct, identity fraud, is the unauthorised use of another's personal information to achieve financial gain.'[166]

Therefore, as the British Home Office correctly defines it, identity theft is 'the act whereby someone obtains sufficient information about an identity to facilitate identity fraud ("ID fraud") irrespective of whether, in the case of an individual, the victim is alive or dead."[167] This definition is useful in two ways. One, it shows, as the OECD itself pointed out, that identity theft is a part of a larger chain of wrong-doing.[168] Two, it confirms that although it may be preparatory or preliminary to the commission of identity fraud, identity theft carries no implication of intention to commit or actual commission of identity fraud. The explicit suggestion is that identifying information be in sufficient proportion to be capable of facilitating identity fraud whether or not fraud subsequently occurs.

Neither identity theft nor identity fraud was specifically mentioned under the Nigeria law. However, theft or stealing is a crime. Under section 383(1) of the Criminal Code Act, 'A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing. Section 383(2), provides additionally that a person who takes or converts anything capable of being stolen is deemed to do so fraudulently if he does so with intent, inter-alia,[169] to permanently deprive the owner or any person who has any special property in the thing of the property.[170] Generally, "property" includes everything, animate or

---

[162] OECD, *Online Identity Theft* (OECD 2009), 16.
[163] Javeline Strategy and Research, '2010 Identity Fraud Survey Report: Consumer Version' 5 <https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraud Survey Consumer.pdf> accessed 21/03/2014.
[164] ibid.
[165] Lynn M. LoPucki, 'Human Identification Theory and the Identity Theft Problem' (2001-2002) 80 Tex L Rev 89, 90.
[166] ibid.
[167]Home Office Identity Fraud Steering Committee (2006) <http://www.bournemouthcrimeprevention.co.uk/download/printableversion.pdf>accessed 11/08/2012.
[168] OECD, *Online Identity Theft* (n 162).
[169] s 383(2)(c)-(f) Criminal Code Act.
[170] ibid s 383(2)(a)-(b).

inanimate, capable of or being the subject of ownership.'[171] Correspondingly, a thing capable of being stolen is every inanimate thing whatever which is the property of any person, and which is movable or capable of being made movable.[172] For the purpose of the offence, it is immaterial that the thing is made movable in order to steal it,[173] but a person shall not be deemed to take a thing unless he moves the thing or causes it to move.[174] Physical objects, animals and other intangible property such as a thing in action are capable of being stolen, whereas land is not capable of being the object of theft.[175] The elements of a theft offence are therefore ownership, fraudulent conversion, movability and indeed moving the property, as well as intent to permanently deprive the owner of the property or the thing in the property stolen.[176]

In creating an offence referred to as 'personation', the Criminal Code Act criminalises the impersonation of another by misrepresenting one's identity with intent to fraud. Section 484 of the Act provides, 'Any person, who, *with intent to defraud any person*, falsely represents himself to be some other person, living or dead, is guilty of a felony'.[177] While it is possible to argue that based on this later provision, identity fraud is criminalised in Nigeria, there is some grey area with respect to identity theft. The question which must be asked here is one which pervades the literature.[178] That is, given the provisions of the relevant law, in this case, the Nigerian Criminal Code, can information (and by extension personal information) be the subject matter of theft?

The Nigerian Courts have not decided this question, but it has been raised and considered by the courts in England. In *Oxford v Moss*,[179] the court had to interpret sections 1 and 4 of the Theft Act in relation to the alleged theft of confidential information. Under section 1, 'A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it'.[180] Section 4(1) provides that "Property" includes money and all other property, real or personal, including things in action and other

---

171 ibid s 1(8).
172 ibid s 382.
173 ibid.
174 ibid s 383(6)
175 ibid s 382.
176 See eg *FRN v Yaro* (2012) 3 SCNJ 236-237.
177 s 484 Criminal Code Act (emphasis).
178 See eg Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data' (2011) 22(1-2) Criminal Law Forum 145.
179 (1979) 68 Cr App R 183.
180 See Theft Act (UK) 1968 s 1.

intangible property.' The facts of the case are briefly that the defendant while a student at a university dishonestly took physical possession of a proof examination question paper. He returned the paper after reading it. He was charged with theft of intangible property, that is, the confidential information on the proof examination question paper, contrary to sections 1 and 4 of Theft Act. The court acquitted the defendant on grounds that confidential information did not fall within the meaning of intangible property under section 4(1) of the Theft Act. According to the court, confidence consisted in the right to control the publication of the proof paper and was a right over property other than a form of intangible property.[181]

Against the background of the above decision and considering the position of the Nigerian law on the elements of the theft offence, one may speculate on the likely outcome of a charge of information theft in Nigeria. In the first place, it is unclear whether courts in Nigeria will define intangible property to include information.[182] However, even if it is assumed that information is (intangible) property, there are other elements of the offence to be considered. The courts have suggested for example that ownership is crucial to a conviction for theft. According to the Supreme Court;

> Ownership is a most vital and indispensable essential or ingredient of the offence of stealing. ... It is the baseline of the offence of stealing. [Therefore,] Before an accused could be convicted of the offence of stealing property, there must be evidence that the property is owned by a person, the person could be a natural person or an artificial person…[183]

It may seem an obvious answer that the owner of personal information is the person to whom the information relates. As McNally argues, identity theft victimises the owner of the identity, whereas the victims of identity fraud are entities or organisations such as banks and credit card issuers who are fooled or deceived by the fraud.[184] Accordingly, the victim of the theft is also the owner of the information. However, under the Nigerian Criminal Code, a person having possession or special interest in the property stolen has the rights of ownership.[185] In effect, personal information on proprietary computers and networks may also be deemed to be the property of organisations. It would therefore seem that along with

---

[181] *Oxford v Moss* (1979) 68 Cr App R 183, 185.
[182] See previous notes in 4.2.2 Hacking as Damage to Property p 93.
[183] *Onagoruwa v The State* (1993) 7 NWLR (Pt 303) 86.
[184] Megan M. McNally, 'Trial by Circumstances: Is Identity Theft a Modern –Day Moral Panic?' (ProQuest LLC 2008) 9.
[185] See s 383(2) (b) Criminal Code Act.

resolving whether information is intangible property, the courts will also have to resolve the question of ownership.

In addition, the law requires that inanimate things capable of being stolen must also be movable or made movable by the thief. Conversely, in data terms, 'theft' may involve the mere copying of the information rather than *taking or moving.* By processes of replication and duplication, data can be 'stolen' even while literally, it remains unmoved. Furthermore, even if moving could creatively be extended to include copying, (as in cases where information is copied from hard drive to flash drive), the fact that the 'thief' has not permanently deprived the owner of the information is arguably fatal to a charge of theft. This is even more compelling when one considers that the information may be backed up. The court in *Oxford v Moss* applied the same reasoning when it held that since taking of the examination paper did not permanently deprive the owner of the intangible property, a material element of the offence was not satisfied.[186] The Nigerian Court of Appeal has also affirmed this position when it held that for the purpose of the theft offence, there must be an intention to deprive the owner permanently of the property or 'animus furundi.'[187]

The conclusions may be drawn therefore, that unless the law adopts a definition which accommodates the peculiarities of information appropriation, the theft of personal information is a legal impossibility. It is however to be noted that in spite of the lacuna that could exist in identity theft cases, much debate still surrounds the criminalisation or otherwise of bare theft of identity. In England for example, there is still no separate or specific offence of identity theft.[188] Identity theft can only be dealt with by the provision of Fraud Act relating to false representation, or because it is a precursor to identity fraud, by the law on criminal attempts, provided clear evidential links exist.'[189] As Finch correctly points out, even in spite of the Fraud Act, bare theft of identity information cannot ground criminal liability.[190] Walden further argues that criminalising identity theft is problematic because the term 'identity theft' is a misnomer since information itself is not generally capable of being stolen.[191]

---

[186] See *Oxford v Moss* (n 181).
[187] *FRN v Yaro* (n 176).
[188] Compare Identity Theft and Assumption Deterrence Act 18 USC 1028.
[189] Ian Walden, *Computer Crimes and Digital Investigations* (OUP 2007) 116.
[190] Emily Finch, 'The Problem of Stolen Identity and the Internet' in Yvonne Jewkes (ed) *Crime Online* (Willan 2007) 29.
[191] Walden, (n 189).

Along similar lines, it has been argued that people do not steal but merely assume false identities.[192] Koops and Leenes argue for example that the term identity theft is misleading as it conjures the image of victims chasing after thieves running away with their identities. As they further argue, identity criminals do not steal identities, in reality, they use identity as a tool to steal money.[193] Therefore, since it is often difficult to establish the fact of identity theft unless and until further (identity) crimes are committed, it seems pointless to criminalise the bare theft of identity information. [194] The further inference here is that in the context of harm and victimisation, identity theft is a sterile terminology. Invariably, if a fictitious or fraudulently obtained identity is never used, then one can argue that the identity was never stolen, even if the information was retained for future criminal use. Perhaps, also taking this view of identity theft, the drafters of the Nigerian Cybercrime Bill refrained from specific criminalisation of identity theft. Under the head identity theft and impersonation, the cybercrime bill provides;

> Any person who in the course of using a computer, computer system or network-
> (a) knowingly obtains or possesses another person's or *entity's* identity information with the intent to deceive or defraud, or
> (b) fraudulently impersonates another entity or person, living or dead, with intent to-
> (i) gain advantage for himself or another person;
> (ii) obtain any property or an interest in any property;
> (iii) cause disadvantage to the entity or person being impersonated or another person; or
> (iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice,
> commits an offence and liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment. [195]

Apart from its criminalisation of the theft and impersonation of the identity of entities other than individuals, which is arguably commendable on account of its usefulness in the areas of spoofing and website cloning,[196] the proposal leaves the position of the law unchanged. In other words, although the offence quoted above is titled identity theft and impersonation, the

---

[192] McNally, (n 184).
[193] Bert-Jaap Koops and Ronald Leenes, 'ID Theft, ID Fraud and/or ID-Related Crime: Definitions Matter' (2006) 9 Datenschutz und Datensicherheit 553.
[194] See eg McNally, (n 184).
[195] s 13 Cybercrime Bill 2014.
[196] For example, this may suggest quite correctly, that the identities of corporate organisations could also be stolen.

proposed law did not infact create an offence of identity theft. With its emphasis on subsequent use such as intent to deceive or defraud, the proposed law merely re-created the impersonation offence which already existed under the Criminal Code. The only difference being its reference to computer systems. Consequently, even under the Cybercrime Bill, bare theft of identity information will not constitute an offence. However, consistent with the definition of identity theft earlier given, and earlier discussion on the risks and justifications for hacking, as well as the analysis of the concept of theft above, the omission to expressly criminalise identity theft may be fatal. For example, the same arguments that 'basic hacking' or mere unauthorised access suffices to ground criminal liability is applicable to theft of identity information as the criminalisation of identity theft may serve as deterrence to other identity related offences.

Furthermore, as the analysis of the theft offence above shows, if a person steals property belonging to another, the law does not require that the item be valuable or that the thief do specified acts concerning the property. It is sufficient merely to establish that the item belongs to another, that it is capable of being stolen and was indeed stolen. By the same token, if a person obtains bank details, PINs, and passwords unlawfully, fraudulently or without authority, he must be deemed to have committed identity theft. We do not have to look further into whether or how he intends to use the information to render him criminally liable. The argument applies with equal force even if the identity is fictitious in the sense that it does not belong to anyone. The analogy must be between a person who stole a gun and another who bought a gun. In both cases, if possession is unlawful, the person who bought a gun even for self-protection is guilty of a crime.[197] Therefore, although the term identity theft may be less apt, if a person obtains a credit card, or a passport or identity document in a fictitious name, he must be deemed to have committed identity theft.

4.6 Administration and Enforcement under the Cybercrime Bill

Administration and enforcement are perhaps the most important aspects of cybercrime legislation. This is particularly so because it is virtually impossible to regulate criminal behaviour unless there is also a means to ensure the enforcement of sanctions.[198] As the analysis above imply, the extant criminal laws in Nigeria contain no specific provisions on cybercrime and therefore no provisions on enforcement. In spite of this position, the

---

[197] See for example the reasoning of the US Supreme Court in *State of North Carolina v Antonio Monroe* (Supreme Court of North Carolina No 153A14 of 15th April 2015).
[198] Amalie M Weber, 'The Council of Europe Convention Cybercrime' (2003) 18(1) Berkeley Technology Law Journal 425.

Economic and Financial Crimes Commission (EFCC) assumes the powers to investigate and prosecute cybercrimes in Nigeria. By its own admission, however, these powers are not specifically conferred by law, rather, the Commission acts pursuant to its general mandate to investigate economic crimes.[199] Accordingly, neither the EFCC nor any other law enforcement agency in Nigeria could lay exclusive claim to powers to investigate cybercrimes.

It is notable that the Cybercrime Bill 2014 maintains the status quo. The bill did not provide for the establishment of an implementing or enforcement agency for the law. It proposes rather to establish a Cybercrime Advisory Council (the Council). The Council shall comprise of a representative each of the ministries and agencies listed under the schedule to the bill.[200] The Council shall have the power to formulate and provide general policy guidelines for the implementation of the law. It shall also have the power to advice on measures to prevent and combat computer-related offences, cybercrimes, threats to national security and other cyber security related issues. The bill further provides that the Office of the National Security Adviser (ONSA) shall be the co-ordinating body for the administration and enforcement of the law. The Council shall meet a minimum of four times a year presided over by the National Security Adviser (NSA).[201]

It is notable that the explanations provided for the above provisions on enforcement include the need to keep the costs of enforcement low, and to facilitate the development of capacity across the broad spectrum of law enforcement in Nigeria as well as the need to address the "fight or battle for turf".[202] In the sections below, it is argued that although these explanations seem rational, they also re-enact the politics and policy inconsistencies which have impacted on the development of the law in the area of cybercrime and cybersecurity in Nigeria.

4.6.1 Lack of Computer Forensics Capacity in Law Enforcement

As stated above, one argument justifying decentralisation of enforcement of the proposed cybercrime law is the need to ensure that each law enforcement agency in Nigeria develops computer forensics capacity. Computer forensics involves the collection, preservation and

---

[199] See s 6(b) & ss 14-18 Economic and Financial Crimes Commission (EFCC) Act Cap E1 LFN 2004; see also EFCC (Establishment) (Amendment) Bill 2010 [HB 351] C 349.
[200] Under the Schedule, virtually all law enforcement agencies in Nigeria and some ministries, and departments (22 in all) will be represented on the Council. See Schedule to the Cybercrime Bill 2014.
[201] ibid ss 25(1), 26(1) (a) –(b).
[202] Policy maker 1, 2, 3.

presentation of evidence derived from information systems in a form which complies with the law and makes the evidence viable or admissible in court.[203] It entails investigators knowing how to identify, intercept or retrieve messages even when they have been deleted, encrypted or hidden in a vast database.[204] Therefore, on account of the technicalities and complexities of information systems, regular law enforcement agents would require further training not only in the technical aspects of the investigation but also on its legal, ethical and regulatory implications. This training has cost and policy implications.

To illustrate, it appears to be accepted that there is lack of capacity in computer forensics across the broad spectrum of law enforcement in Nigeria. [205] According to a policy maker, due to this capacity deficiency, the Cybercrime Prosecution Unit set up in 2010 is yet to undertake a single prosecution to date.[206] As he further argues, this is because there is only a "pocket of experts" within the law enforcement while there are virtually none within the judiciary.[207] Also according to a law enforcement agent, most computer forensic experts, including himself, have achieved forensic expertise only through personal efforts and personal funds.[208] The suggestion here is that government has not invested in the training of the existing "pocket of experts" so far. If this assumption is correct, then one must ask whether, considering its cost implications, it is realistic or even reasonable to assume that government would invest in capacity development across the broader spectrum of all law enforcement agencies in Nigeria as anticipated by the drafters of the Cybercrime bill.

One may argue further that since computer forensics is both specialised and technical, and most agencies already have their core speciality,[209] it may be difficult to see how different agencies could develop capacity to an efficient or proficient level to investigate and prosecute cybercrimes. In other words, even if in theory, it is possible for every law enforcement agency to embark on training and capacity development for investigation and

---

[203] See US Cert, 'Computer Forensics' (2008) <https://www.us-cert.gov/sites/default/files/publications/forensics.pdf> accessed 01/04/2015.
[204] Jerry Wegan, 'Legal Issues in Computer Forensics' (2004) 8(1) Proceedings of the Academy of Legal, Ethical and Regulatory Issues 45.
[205] Although usually with the objective of shifting the responsibility for training elsewhere, all stakeholders including law enforcement agents, IT security experts, regulators and service providers made this observation.
[206] That is as at June 2013 when the interview was conducted.
[207] Policymaker 2.
[208] Law enforcement 2.
[209] For example, the EFCC was set up to combat economic crimes including money laundering, the National Drug Law Enforcement Agency (NDLEA) was set up to investigate drug trafficking and other drug related offences, the National Agency for the Prohibition of Trafficking in Persons (NAPTIP) has as its core speciality combatting child and people trafficking and so on.

prosecution of cybercrimes, one could argue that this would create a "Jack of all trades" situation where capacity exists but at superficial and incompetent levels. Perhaps for similar reasons, lawmakers argued against the designation of the ONSA as the co-ordinating agency for the cybercrime law during their debate of the Cybercrime Bill. As the lawmakers argued, 'The National security Adviser is not a Minister; his office is not a Ministry or an Institution…That is the status of the National Security Adviser. It is not an institution…that we can confer statutory duties upon…'[210] According to another lawmaker, '…it looks like we are overburdening the National Security Adviser's Office with crime prevention and control. Therefore, we are transforming that office into something that it is not intended to be.'[211] It is remarkable that in spite of these observations, the enforcement provisions in the bill were retained. Nevertheless, the observations underline both the perceived incompetence and expected inefficiency of the ONSA as an advisory council in the place of a cybersecurity agency.

Finally, in addition to lack of capacity, there also appears to be lack of consensus on whether and when government should commence capacity development in computer forensics. On the one hand, it was suggested that capacity development should commence regardless of passage of a law on cybercrimes.[212] On the other hand, it was argued that capacity development in lieu of legislation is anticipatory and therefore wasteful.[213] Applied to the context of enforcement, one would argue that these positions imply that the capacity gap would further deepen while legislation is anticipated or even that capacity development would never commence unless a cybercrime law is passed.

4.6.2 The Politics of the "Fight for Turf"

The empirical data further suggests that decentralised approach to enforcement and omission to create a central cybercrime or cybersecurity agency is a deliberate attempt to address problems associated with the "fight for turf or battle for turf" among law enforcement agencies in Nigeria. Battle for turf describes 'in-fighting' among law enforcement agencies who each want to be empowered to the exclusion of others to investigate and prosecute cybercrimes.[214] The motivation for the fight is perceived "esoterism" of cybercrime and expectations of government funding for any agency

---

[210] Senate Hansard, vol 1 No 27 of Thursday 23rd October 2014, 17.
[211] ibid.
[212] Policy maker 1, 2.
[213] Law enforcement 3.
[214] Policy maker 2, policy maker 1 also refers to the fight for turf as "agency ego".

mandated to enforce the cybercrime law.[215] On account of the fight for turf, the success of a cybercrime bill passing into law depends on whether it purports to confer implementation and enforcement powers on certain agencies to the exclusion of others. Invariably, if the agencies involved in the fight believe a proposal for law fails to take account of their interests, they "lobby" law and policy makers so that the bill is abandoned as early in the law-making process as possible.[216]

Therefore, by refraining from designating an implementing agency, the Cybercrime bill 2014 aims to eliminate the fight for turf. In other words, since all law enforcement agencies would have equal powers to implement the law, none could claim it as its exclusive reserve and none could allege it was excluded. While this approach appears logical, the logic is undermined by the fact that the approach fails to take account of the rivalry which may result when respective agencies implement the same the law. For example, different agencies may withhold critical intelligence information on the basis that a particular aspect of cybersecurity is also their turf. The critical point therefore is that the enforcement provisions in the law and justifications for the provisions overlook the cost implications of computer forensics trainings and the technical nature of cybercrime investigations, as well as the 'politics' (of turf) which have inhibited the development of the law in the first place.

Conclusion

The foregoing analyses demonstrate that the Nigerian criminal law is inadequate to address cybercrimes that threaten e-payment systems whether they are crimes using the computer or crimes of computer misuse. The analyses of specific cases also show that the courts in Nigeria have had little opportunity to test the applicability of the criminal law to cybercrime. The arguments support the proposition that because of the unique dimensions of traditional crimes on the internet, they need to be regulated, along with technology-specific crimes, by separate legislation other than those dealing with conventional theft or fraud.

The examination of the provisions of the proposed law, the Cybercrime bill 2014, also identified the specific arears where gaps exist or where interpretational challenges may defeat the purpose of the law. It was pointed out in particular that significant improvements were not implemented by the proposed law regarding the criminalisation of phishing and

---

[215] Policy maker 2.

[216] There is no clear agreement on what lobby means here. It was argued by some stakeholders that it entails offering financial and other incentives to lawmakers while the lawmakers themselves contend that it only means convincing lawmakers to support an ideological or policy position through arguments and representations. See for example (n 19) at p 11.

identity related crimes on the internet. Moreover, discussions in the chapter imply that while it is arguably useful to have legislation to punish cybercriminals, issues related to societal tolerance of cybercrime, the jurisprudence of crime and punishment, peculiarities of internet transactions and enforcement challenges may inhibit the effectiveness of criminal legislation.

Corresponding to the need to punish cybercriminals, there is a need to limit opportunities for the crime in the first place. To this end, chapter five evaluates alternative legal measures to control cybercrimes. In the context of e-payment systems and services, this involves an examination of data protection standards and practices in sectors and organisations prone to criminal compromise of consumer payment data.

Chapter Five

Data Protection in Nigeria

Introduction

In chapter three, it was argued that both individuals and organisations are susceptible to criminal attacks for information which may be used for identity fraud. While criminals leverage social engineering tactics to obtain information from individuals, they use technical means such as hacking to compromise computer and network systems of payment service providers. As also argued in chapter three, hacking could result in potentially large scale identity theft and fraud and measures such as the PCIDSS are intended to reduce payment card fraud by improving the security of card holder data. The final part of the chapter however pointed out that data security standards are aimed at security breaches generally while data protection laws regulate the protection of personal data which may be used for identity-related crimes.

This chapter examines the legal and regulatory frameworks for data protection in Nigeria. The chapter starts with a brief examination of the privacy and security implications of data processing activities that relate to e-payment systems. It then considers the state of the Nigerian law on data protection generally. In this respect, it examines the provisions of the constitution and guidelines on data protection in the banking and telecom industry. It also examines relevant provisions of a draft law on data protection in Nigeria which is modelled closely to Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) 2000.

The chapter concludes that regulation of data processing is inadequate and ineffective in Nigeria because law and regulation have failed to clearly articulate the nature of the information subject to data protection. Law and regulation have also failed to set out uniform principles on data protection and provide for enforcement measures which could make laws effective in the multi-stakeholders' environment of e-payment services.

5.1 Challenges of Data Protection in E-payment Systems in Nigeria

Two fundamental privacy concerns are associated with users' information in electronic transactions. The first relates to the ways in which the collection, processing, and use of personal information in computer-networked environment contribute to the loss of

individual power and autonomy.[1] This view considers the effects of data processing on the individual's inalienable and fundamental right of privacy. Privacy in this context is viewed as an end in itself.[2] In other words, it entails a subjective privacy right or interest where a person desires privacy irrespective of whether he is harmed by any intrusion. This approach to privacy is essentially intuitionist.[3] Abusive market practices such as direct marketing is an example in this respect. As Clarke argues, the interest in this form of privacy relates to the intrusion inherent in most direct marketing techniques.[4] Arguably therefore, while the activity is not inherently harmful, it is intuitively invasive, and concerns arise regardless of harm or the absence thereof.

The second concern, which is of particular relevance to this thesis, focuses on the detrimental effects arising from processing of personal information. This includes the possibilities of organisational misuse and third party access.[5] One may consider in this respect, sale of consumer information by collecting or processing organisations, or theft and fraud arising from data breaches. In effect, the possibility of misuse, theft, loss or unauthorised access to information by sophisticated hackers raises equally fundamental privacy issues. As noted in a British government White Paper, the principal potential dangers posed by computerised systems to privacy include the possibility of access to personal information by people who should not or need not have it. It also includes the possibility of using the information for purposes or in the contexts other than for which it was collected.[6] Concerns in this respect are often associated with security of the data, and possibilities of misuse and theft rather than simply privacy for its own sake.

Corresponding to the above, the broad issues that generate concerns in Nigeria are the collection of personal information across multiple organisations in the private and public sectors. In the context of e-payments, this is reflected in the multi-stakeholder and multi-provider approach to the provision of e-payment services and the interconnection among the organisations providing the services already discussed in chapter two. The analysis

---

[1] See eg Oscar H Gandy, Jr. 'Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace' (1996) U.Chi. Legal F. 77.
[2] See eg Richard Posner, 'Privacy, Surveillance and the Law' (2008) The University of Chicago Law Review 245.
[3] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale Law Journal 1151, 1154-5.
[4]Roger Clarke, 'Direct Marketing and Privacy' (1998) <http://www.rogerclarke.com/DV/DirectMkting.html> accessed 21/11/2013.
[5] Daniel J.Solove, 'Identity Theft, privacy and the Architecture of Vulnerability' (2002-2003) 54 Hastings Law Journal 1227.
[6] Secretary of State for the Home Department, *Computers and Privacy* (Cm 6353, 1975) para 8.

here further demonstrates that broader processing activities, whether proximate or seemingly unconnected to e-payments, have implications for identity related crimes in e-payment systems. Three separate but interrelated developments particularly contextualise the problem. The first concerns the National Identity Management Commission's (NIMC) National electronic identity card system. The second relates to the Nigeria Communications Commission (NCC) Subscriber Identity Module (SIM) registration project, and the third is Central Bank of Nigeria (CBN) Bank Verification Number (BVN) system.

5.1.1 NIMC's Electronic National Identity Card

The National Identity Management Commission (NIMC) is the central identity management authority in Nigeria. As part of its identity management program, the Commission launched a general multi-purpose electronic identity card and the assignment of National Identification Numbers (NINs). The proposed identity card will contain 13 applications (applets) and will offer PIN and fingerprints authentication, digital signature and payment functionalities.[7] The NIN shall be used mandatorily, among other things, for opening individual and personal accounts and in all consumer credit transactions.[8] The NIMC's value proposition for the financial services industry also includes the use of the national e-identity card as bank card and access by financial institutions to its personal information depository, the National Identity Database (NIDB). The NIDB would presumably be the largest identity database in Nigeria.

The identity card project itself has been lauded as 'one of the most sophisticated smart card projects to date',[9] however, it raises questions about fraud and security. For example, a national identity card enabled with-payment capabilities could contain all kinds of identity related information. Also, considering the NIMC's value proposition, if both the card and the NIMC database could be accessed by different payment and non-payment organisations, it can be argued that it would be difficult to determine whether organisations are able to access only information necessary for the provision or delivery of specific services or whether they can access all personal information stored on the card. It may also

---

[7] See NIMC, 'Facts about the National e-ID Card' <https://www.nimc.gov.ng/?q=facts-about-national-e-id-card>accessed 12/04/2015.
[8] See ss 27, 28, 29 Nigerian Identity Management Commission Act (NIMCA) 2007.
[9] See 'NIMC Nigeria includes identity and payment on the same card, thanks to NXP Semiconductors, MasterCard and SPS' <http://www.prweb.com/releases/2013/11/prweb11329639.htm> accessed 13/03/2014.

be difficult to establish whether such organisations subsequently misuse the information, by marketing or otherwise trading in it. [10]

Furthermore, since the law mandates the use of the card for offline and online identification purposes, the increased link between offline and online identities makes identity theft and fraud easier. As noted in chapter three, access to the card or information on the card can facilitate identity fraud.[11] Therefore, the NIMC's identity card and central database could provide an access point in a way which put users' personal (financial) information at risk of theft. In a research into the risks of a national identity database for the UK,[12] similar observations were made as follows:

> The lack of constraints on the misuse of National Identity Register-derived data once it has been obtained has serious implications…anyone who obtains National Identity Register data is in an ideal position to produce false documents that can be used as a starting point for "identity theft". Far from undermining identity-based crime, the National Identity Register could easily facilitate it.[13]

5.1.2 NCC SIM Registration

The Nigerian Communication Commission (NCC) is the regulatory body for the telecom industry in Nigeria. In 2011, the Commission launched a SIM registration exercise which entails the collection of the names, addresses, gender, date of birth as well as the capture of photograph and fingerprint biometric of SIM subscribers by mobile network operators (MNOs). [14] This development is significant for two reasons. One, prior to the process, such large volume of data about individuals have not been collected or collated in privately operated databases. Therefore, in general terms, the attendant risks of the exercise have not be analysed or accessed. Two, and specific to e-payments, with the introduction and adoption of mobile banking, phone numbers have become increasingly associated with account and other financial information. For example, in mobile payment systems, mobile

---

[10] See observations made earlier regarding trading in personal information, see notes in (e) Smishing/ Vishing at p 65.
[11] See notes in 3.3.1 What is (Digital) Identity? p 52 particularly at 54.
[12] See Identity Cards Act 2006 c 15.
[13] Simon Davies, Ian Hosein & Edgar A Whitely, 'The Identity Project; An Assessment of the UK Identity Cards Bill and its Implications' (The LSE Identity Project Report 2005) 196, <http://eprints.lse.ac.uk/684/1/identityreport.pdf>accessed 11/04/2015.
[14] See Nigerian Communications Commission's Draft Regulations for the Registration of All Users of Subscriber Identity Module (SIM) Cards in Nigeria 2010.

phone numbers operate as second factor authenticator.[15] In addition, banks use phone numbers to send transaction notifications to their customers, both to alert the customers of the most recent transactions and to reduce the incidence of fraud.[16]

However, in spite of the new uses of phones numbers for financial transactions and the attendant possibilities of fraud, MNOs and banks do not attach the same importance to phone numbers. On the one hand, MNOs seem to operate under the assumption that they have proprietary rights over issued numbers and may re-assign telephone numbers at will and without notice to registered subscribers. On the other hand, bankers, who are traditionally obliged to protect their customers' financial information,[17] regard such information as personal. This position indicates that without legal guidance, different views about the value of user information would lead to reduced protection across different sectors involved in the provision of e-payment services.

An example cited by a service provider underline the problems which may arise here. According to the provider, a mobile phone service provider had re-assigned a bank customer's phone number to another subscriber while he (the customer) was outside the country, and because the number had remained inactive for 6 months. Meanwhile, the (customer's) bank continued to send transaction notifications on the account to the telephone number which now ostensibly belonged to a new subscriber. The customer complained about the possibility that the bank had been disclosing his account information to another person and alleged that this could lead to fraud. The bank on its part insisted that the fault (if any at all) lay with the mobile service provider which disconnected the customer without notice.[18] This case exemplifies the links between a phone number and bank details. In the context of identity-related cybercrimes, the case highlights the threats of SIM swap discussed in chapter three.[19]

5.1.3 CBN Bank Verification Number (BVN)

The Bank Verification Number (BVN) is a relatively recent initiative of the CBN. It requires banks to enroll their customers' biometrics for identification purposes. Registration for biometrics includes the capture of facial image, the 10 fingerprints and other unique features of the individual. After registration, customers are issued BVNs. The

---

[15] See previous notes on (a) *Authenticating Technologies* p 76 at 77.
[16] See notes in (e) Smishing/ Vishing p 65 at 66.
[17] This is often based on the recognition of the common law duty of secrecy, see for example *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.
[18] Payment service Provider 3.
[19] See notes in 3.4.4 SIM Swap Fraud p 72.

BVN is a uniform and single identity that will be acceptable across the Nigerian financial system as all bank accounts operated by any individual will be tied to the individual's unique BVN.

The approach is positive in that Nigeria is the first country to implement such a project on a national scale to combat identity related crimes in payment systems, however, it also raises questions about how personal information would be secured. For example, collection of personal information by different banks implies the existence of multiple databases with attendant security problems. As the UK Information Commissioner's Office observed, 'The more databases that are set up…, the greater the risk that the information will be lost, corrupted or misused.'[20] It is arguable that considering attendant issues of cost and size, the safeguards applied to the information would differ even across the financial sector. Consequently, user information may become more accessible to criminals in organisations without standard and effective safeguards.

Generally therefore, because e-payments are integrated and interconnected multi-provider systems, the protection of consumer data must be addressed in a uniform or comprehensive way. It is argued in the remaining part of this chapter that resolving the challenges of data protection centre on answering three questions. One, what is the meaning and scope of the concept of "personal information" in Nigeria. Two, are there general or uniform principles for protecting personal data? Three, what mechanisms are in place for ensuring effective and efficient implementation of data protection standards?

5.2 Regulation of Data Processing in Nigeria – Laws, Regulations and Guidelines

It is important to note from the outset that Nigeria has no general law on data protection. There are however provisions in the constitution relating to the general area of privacy and certain aspects of information privacy. The telecommunications and banking sectors also provide data processing guidelines for organisations in the respective sectors. A proposal for a generally applicable data protection law, the Information Privacy and Data Protection Bill 2013 was drafted by the Nigerian Identity Management Commission in 2013 but was not debated by the Nigerian National Assembly. The analysis that follows examines the scope of the constitution, industry regulations and guidelines, as well as the proposed law.

[20] http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_7 accessed 13/03/2014.

5.2.1 Constitutional Provisions on Privacy Protection

As mentioned above, the Nigerian constitution contains provisions which cover the general rights of privacy. Section 37 of the Constitution provides, 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'[21] Although, the provision contains reference to specific aspects of information privacy, that is correspondence, telephone conversations and telegraphic communications, the constitutional provision does not cover data protection. This assertion can be supported by highlighting the distinctions between privacy and data protection.

5.2.1.1 Distinguishing Data protection from Privacy

Bygrave defines data protection as a set of measures (legal and non-legal) aimed at safeguarding persons from detriment resulting from the processing of (computerised or manual) information on them. [22] According to Kuner, 'Data protection …is a specific aspect of privacy that gives rights to individuals in how data identifying them or pertaining to them are processed, and subjects such processing to a defined set of safeguards.'[23] The Committee on Data Protection described data protection as a set of legal framework aimed at safeguarding personal data.[24] From these definitions, components implicated in data protection include privacy protection, personal data, and legal safeguard for protection.

Most legislation on data protection often establishes the links between privacy and data protection.[25] As examples, the objective of the EU Directive on Data protection was to ensure that member states protect the fundamental rights and freedoms of natural persons, and in particular their right to *privacy* with respect to the processing of personal data. [26] Similarly, the purpose of the proposed data protection law in Nigeria is to establish rules to govern the processing of personal information in a manner that recognises *the right of*

---

[21] s 37 Constitution of the Federal Republic of Nigeria (CFRN) 1999.
[22] Lee Bygrave, 'Data Protection Law: Approaching its Rationale, Logic and Limits' (2002) The Hague: Kluwer Law International 23.
[23] Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law' (OECD Digital Economy Paper No. 187 2011), 13.
[24] *Report of the Committee on Data Protection* (Cmnd 7341, 1978) para 2.05-2.13.
[25] See eg Council of Europe Convention for the Protection of the Individual with regard to Automatic Processing of Personal Data (ETS no 108) 1981 (hereinafter Convention ETS no 108); see also Council Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data [1995] OJ L281 (hereinafter Directive 95/46/EC).
[26] See Directive 95/46/EC, art 1; see similar provisions in Convention ETS no 108, art 1.

privacy of individuals with respect to their *personal information.*[27] On account of this relationship with privacy, it is usual for data protection to be used synonymously with privacy.[28] However, it has been noted that this near universal consensus, that privacy is synonymous with data protection, is both misleading and questionable. [29] As Kuner observes, although the concepts are related, they are not synonymous. [30] Hert and Schreuders describe the concepts as 'twins but not identical.'[31]

The conceptual and theoretical arguments in this area surround the notion that while data protection is inescapably grounded in the jurisprudence of privacy, it (data protection) is not wholly about privacy and is a concept both wider and narrower than privacy. Kuner argues that under European law, privacy is a broader concept because it includes issues relating to the protection of rights unrelated to data protection such as personal or physical space, family and home life, moral integrity, honour, and reputation.[32] The Committee on Data Protection in England also puts the distinction in clear perspective when it noted;

> There are aspects of privacy which have no immediate connection with the handling of personal data in information systems, such as intrusion into the home, power of entry and search, and embarrassing publicity in the media. There are also aspects of data protection which have no immediate connection with privacy. For example, the use of inaccurate or incomplete information for taking decisions about people is properly a subject for data protection, but it may not always raise questions of privacy.[33]

In other words, privacy is broader because it serves a range of other values and interests apart from data protection.[34] In contrast, the object of data protection, personal data, is distinct and separable. The aspect of data protection which relates to privacy, rightly referred to as data privacy by the Data Protection Commission in the UK, deals with how the handling of personal information by information systems impacts on the privacy of the

---

[27] See s 1 Personal information and Data Protection Bill 2013(emphasis added)
[28] Kuner (n 23).
[29] Lee Bygrave, 'The Place of Privacy in Data Protection Law' (2001) 24(1) UNSW Law Journal, 277.
[30] Kuner (n 23).
[31] P de Hert and E Schreuders, 'The Relevance of Convention 108' (Council of Europe Conference on Data Protection, Warsaw, 19-20 November 2001) cited in Christoper Kuner, *European Data Protection Law* (2nd edn, OUP 2007) 2.
[32] ibid (Kuner), 3.
[33] *Report of the Committee on Data Protection* (Cmnd 7341, 1978) para 2.03.
[34] see eg Durant v Financial Services Authority [2003] EWCA Civ 1746.

individual.[35] Privacy in this sense clearly refers to protection from possibilities of misuse, loss or theft of the individual's personal information.

The distinctions between privacy and data protection underline the limits of section 37 of the Nigerian constitution quoted above. It can be argued for example that by enumerating specific areas of information privacy, that is, *correspondence*, *telephone conversations* and *telegraphic communication*, the Nigerian constitution overlooks the plenary of information which may require legal protection. As shown by the foregoing analysis, this includes personal information. The foregoing discussion also demonstrates that the constitution only articulates a general right of privacy of the individual to keep certain information private. It does not extend to the right to regulate access to that information when it has been disclosed. It follows therefore that unlike general rights of privacy which may be subjective, (in that a person determines what is private to him), data protection prescribes objective standards for protection for information categorised as personal.

The above distinction is also particularly useful because it establishes the underlying rationale for data protection in the first place. For example, it demonstrates that individuals seldom possess the right or ability to decline disclosure of personal information when engaged in certain forms of transactions. In effect, the question is not so much whether consumers should disclose personal information or whether organisations' are able to collect it, but whether the consumers want the particular service. [36] In view of this position, data protection laws create corresponding obligations to regulate the use of the information which consumers must disclose. Put more explicitly, the implementation of data protection laws does not strictly prohibit the processing of information but rather restricts the ability of people and organisations to gain access to information about others. Accordingly, data protection laws decrease the chances of pervasive information collection and illegal or unauthorised access to personal information. It does not confer a right on a person to withhold the information altogether, and it is on this basis that data protection is referred to as Fair Information Practices or (FIRs).[37]

This view of data protection is consistent with developments in technology and the demands of economic growth. As Lord Norman aptly noted;

---

[35] Norman Lindop, 'Legislating for Data Privacy' in Colin Campbell, (ed.) *Data Processing and the Law* (Sweet and Maxwell 1984) 155, 157.
[36] South African Law Reform Committee, *Privacy and Data Protection* (Paper 109 2005) 5.
[37] See eg Paul M Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices' (2000) Wis L Rev 743.

> It is the nature of modern society that the individual, in return for goods and services and in the expectation of continued support, voluntarily gives information about himself to those agencies and organisations who can offer him these commodities. Often he must be aware that information will pass into highly sophisticated networks, the existence of which and the capacity of which may be outside his direct experience or even beyond his understanding; the acceptability of the social transaction to the individual must be based on the fundamental confidence which he has that the organs of society will deal justly with him and that his relative impotence will not be exploited.[38]

From the foregoing, it can also be inferred that another objective of data protection is balancing the respective interests of individuals and the requirements of legitimate businesses with regard to personal information. The Council of Europe Convention reinforces this notion when it enjoined member states to adopt laws which protect the interests of data subjects (individuals whose data is being processed) while advancing legitimate interests of businesses.[39] As observed in the Convention, restrictions on flows of personal data could cause serious disruption in important sectors of the economy, such as banking. [40] Accordingly, to ensure efficient conduct of industry, commerce and administration, it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information.[41]

Data protection is therefore distinct form privacy not only because it encompasses interests which are not necessarily 'private' but also because it creates a legal framework for balancing individual rights to information privacy and the legitimate interests of businesses' need to know. This distinction further underlines the limitations of organisational data security standards and practices examined in chapter three. As noted in that chapter, data security is served by organisational and technical measures. These measures protect data itself irrespective of its content or the legal qualification, and are not necessarily focused on protection of personal data. Encryption for example will protect any content whether personal information, payment instruction or as depicted in the MItM attacks, even criminal content.[42] In contrast, Data protection laws require the standard of protection for a specific category of information, that is, personal information. Therefore, the distinctions

---

[38] Lindop, (n 35), 157.
[39] See Preamble to Convention ETS no 108.
[40] ibid.
[41] ibid.
[42] See previous notes on (d) Public Key Infrastructure (PKI) p 82.

further reinforce the notion that in Nigeria, technology is not an alternative to, but complementary of legislation.[43]

5.2.2 Freedom of Information Act 2011

The Freedom of Information Act (FOI) 2011 is another law which purports to protect personal information. The FOI protects official personal information held by public institutions. Although the law defines personal information, the definition is narrow and applies specifically to public authorities.[44] The most outstanding provision of the law require public institutions to deny any application for information that contains personal and other information exempted under the law.[45] Beyond this provision, the FOI Act does not contain specific principles for regulating data processing by public institutions to which it applies and does not confer enforcement powers on any authority.

5.2.3 Guidelines on Data Processing in Telecom and Banking Sectors

Both the Nigerian telecommunication and banking industry provide guidelines on data processing. Part VI of the Nigerian Communications Commission Consumer (NCC) Code of Protection Regulations, titled "Protection of Consumer Information" sets out data processing rules for NCC licensees.[46] Under the Regulations, NCC licensees are required to conform to the following data protection principles;

(a) Fair and lawful collection and processing
(b) Processing for limited and identified purposes
(c) Personal data to be relevant and not excessive
(d) Personal data to be accurate
(e) Personal data not to be kept longer than necessary
(f) Processing in accordance with the Consumer's rights
(g) Protection against improper or accidental disclosure; and
(h) Transferability of personal data to third party[47]

---

[43] See further notes in 6.4 The Limits of Technology, Industry and Users in Controlling Identity-related cybercrimes in e-payment systems in Nigeria p188.
[44] See further notes below in 5.3 Meaning and Scope of Personal Information in Nigeria.
[45] See s 14(1) (2) Freedom of Information Act 2011.
[46] See s 35 Nigerian Communications Commission Consumer Code of Practice Regulations (Federal Republic of Nigeria Official Gazettee Vol 84 No 87 of 10th July 2007) (hereinafter NCC Code of Practice Regulations).
[47] ibid 35(1) (a)–(h).

Similarly, the Central Bank of Nigeria (CBN) Guidelines on Electronic Banking provides that banks should protect the 'privacy' of the customer's data by applying the following principles:

(i) that customer's personal data are used for the purpose for which they are compiled.

(ii) consent of the customer must be sought before the Data is used

(iii) data user may request, free of cost for blocking or rectification of inaccurate data or enforce remedy against breach of confidentiality

(iv) processing of children's data must have the consent of the parents and there must be verification via regular mail.

(v) strict criminal and pecuniary sanctions are imposed in the event of default.[48]

It is important to mention here that the two guidelines only state data processing principles in sparse terms. For example, they contain no accompanying explanations in terms of what the principles mean or the conditions for assessing whether organisations are in compliance. Generally principles of data protection set the standards which organisations, and sometimes government must comply with in processing personal data. The principles often center on ensuring data quality, data security, and lawfulness as well as transparency or fairness of data processing.[49] In the context of identity-related crimes, principles such as safeguard requirements will prevent unauthorised or criminal access to personal information held by organisations. Principles such as purpose identification, lawful processing of data and consent will also check organisations' misuse including sale or transfer to third parties or even accidental disclosures. The principles are therefore fundamental when considered from the perspective that both payment service providers and non-service providers collect large volume of user information which may be used for identity-related cybercrimes. However, to be effective, the principles have to be clearly set out and the rights, duties and obligations of the parties must be explained to outline responsibility and accountability. This guidance is lacking in the industry guidelines highlighted above.[50]

---

[48] See item 3.0(d) (ii) CBN E-banking Guidelines.

[49] See eg Directive 95/46/EC, see also the African Union Convention on Cybersecurity and Personal Data Protection (African Union Instrument LC12490 (2014).

[50] Compare the provisions of the Data Protection Act 1998 (UK) pt I sch I & Pt II sch 1.

In addition to the above, the Central Bank of Nigeria (CBN) and the Nigerian Communications Commission are the regulatory or enforcement authorities for the purpose of ensuring compliance with the principles. However, apart from vague references to penalties, there is nothing in both regulatory frameworks to suggest robust enforcement of the industry data protection guidelines. Under the E-banking guidelines for example, it was simply stated that, 'Banks should protect the privacy of the customer's data by ensuring: strict criminal and pecuniary sanctions are imposed in the event of default.' [51] The provision does not define the nature of the criminal sanction or the offence a person may be charged with. The extent or limit of the pecuniary damage is also not spelt out. More fundamentally, the provision seems to confer the right to impose sanctions on the organisations to which the Guidelines apply rather than vesting the Regulator (CBN) with the power. Based on the wordings of the Guidelines therefore, it is the banks that should ensure protection and at the same time they are the ones to impose criminal and pecuniary sanctions upon default. [52] This appears contradictory of the essence of regulation because the effect would be to render an organisation both the defendant and the arbiter in its own case.

Even if an alternative interpretation is applied, as for example that the bank is to apply criminal or pecuniary sanctions against an officer (of the bank) directly guilty of the default, the effect is the same. As already argued in chapter three, banks seldom admit to any form of liability or breach of data. The question then is whether it is reasonable to expect the same organisations to impose punishment or penalties on themselves. Therefore, against the background of the wording of the regulatory guidelines alone, it is possible to argue that there is failure of regulation in the area of data processing as far as the banking sector is concerned.

Under the NCC Regulatory Instrument, Nigerian Communications Commission Consumer Code of Practice Regulations, the power to regulate and impose sanctions is clearly placed on the Regulator. The Regulations provide:

> Any Licensee that contravened any of the provisions of these Regulations is in breach thereof and is liable to such fines, sanctions or penalties, including any penalties determined under the Nigerian Communications (Enforcement

[51] Item 3.0(d), (v) CBN E-banking Guidelines.
[52] ibid.

Processes, etc.) Regulations 2005, as may be determined by the Commission from time to time.[53]

It provides further that the Commission will monitor compliance with the Code on a regular basis and publish quarterly reports of identified breaches and the remedial action taken with respect to such.[54] The Commission will also investigate consumer and industry complaints regarding compliance with its data protection rules and other provisions of the code.[55] The only offence recognised with respect to data processing is under the SIM registration regulation of the NCC which penalises contravention of the purpose limitation requirement.[56]

It is notable that regulatory powers under the NCC Consumer Code are more comprehensive than under banking guidelines. However, it is unclear whether the provisions are effective. For example, no evidence could be found of the NCC's published report on data breaches. It must therefore be assumed that it is either there has never been a breach of this regulation or that regulatory oversight is ineffective.

5.2.4 Draft Law on Data Protection- Information Privacy and Data Protection Bill 2013

A Bill titled Information Privacy and Data Protection Bill 2013 (hereinafter draft law) proposes to regulate the processing of Personal Information of Individuals by organisations other than government institutions.[57] The draft law is modelled on the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) 2000,[58] It contains ten principles of data protection and makes provisions for the establishment of a Privacy Protection Office and the appointment of a Privacy Commissioner vested with certain functions and powers.[59] Processing by government institutions, by individuals for domestic purposes, and for journalistic, artistic or literary purposes are exempted from the operation of the law.[60] Although, as noted above, the bill was never debated, and there is some doubt

---

[53] s 9 pt I NCC Code of Practice Regulations (n 46)
[54] ibid s 51 pt II.
[55] See s 52 pt II Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (hereinafter NCC SIM Registratration Regulations).
[56] ibid s 21(1).
[57] See long title to the Personal Information and Data Protection Bill 2013; see also s 2(1), (2).
[58] See Personal Information Protection and Electronic Documents Act (PIPEDA) SC 2000, c 5 current to November 2013.
[59] See sch 1 & s 4 Personal Information and Data Protection Bill 2013.
[60] ibid s 2(2) (a)-(c).

that it was ever presented to the National Assembly, its provisions offer an understanding of the direction of law and policy in the area of data protection in Nigeria, and are referred to as necessary in the analyses that follow.

5.3 Meaning and Scope of Personal Information in Nigeria

It was noted earlier in chapter three that the determination of what constitutes personal information is fundamental to how and whether organisations protect specific types of (personal) information or a broader category of information which may be classified as identity information.[61] Personal information is therefore the central concept of data protection. Its significance lay in its use for identification purposes and the potential misuse for identity related crimes. However, while the terms personal data or personal information is used frequently, and often presumptuously, its meaning is neither obvious nor static. As Professor Kang noted, personal information is the central component of all definitions of information privacy, yet it is the 'the least self-explanatory'.[62] In order to argue intelligibly about how to protect personal information therefore, it is necessary to define the concept and its scope.

5.3.1. Definitions of Personal Information under Laws and Regulations in Nigeria

Two laws and a regulatory instrument define personal information in Nigeria. The Freedom of Information (FOI) Act defines personal information as 'any official information held about an identifiable person, but does not include information that bears on the public duties of public employees and officials.'[63] As noted above, the FOI Act is mainly directed at information processing by public institutions and is not comprehensive.

The Nigeria Identity Management Commission (NIMC) Act defines personal information as a person's full name, other names by which the person is or has been known, date of birth, place of birth, gender, address of the individual's residence in Nigeria and address of every other place in Nigeria where the individual has a place of residence.[64] Identification information is photographs of the individual's head and shoulders, the individual's signature, fingerprints and other biometric information about the individual.[65]

---

[61] See also previous notes in 3.3.1 What is (Digital) Identity? p 52 at 55.
[62] Jerry Kang, 'Information Privacy in Cyberspace Transactions' (1998) 50(4) Stanford Law Review 1193, 1206.
[63] s 30(3) Freedom of Information Act 2011.
[64] See second Sch para 1 Nigeria Identity Management Commission (NIMC) Act 2007.
[65] ibid second Sch para 2.

The definition adopted in a regulatory guideline by the Nigerian Communications Commission (NCC) follows only a slightly different track. Under the NCC Regulations, "personal information" refers to the full names (including mother's maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such *other* personal information and contact details of subscribers specified in the Registration Specifications.' [66] The regulations define "Registration Specifications" as the Data Dictionary, Guidelines on Fingerprint Quality, specifications for Digital Image Standards and Quality, the XML Schema, Transmission protocol and the Technical Interface specifications and such other specifications and amendments that may be made or issued by the Commission, from time to time to guide the registration of subscribers and the interaction of Licensees.[67] In effect, personal data is very much what the NCC regards as personal information and applies to the narrow area of telephone subscribers' registration.

The above definitions indicate that laws and guidelines in Nigeria adopt different approaches to defining personal information. Although, it is arguable this was intended to reflect the types of personal information with which respective sectors or industry deals, the differences in definitions highlight two problems. One, it suggests the delimitation of the notion of personal information in respective sectors. Two, it implies that in sectors, such as the banking industry, which has no definition of personal information at all, the determination of what constitutes personal information may be left to individual organisations. This approach produces relativity and justifies the application of different security standards to the same information in different sectors or even within the same sector.

Conversely, since the draft law on data protection proposes to regulate data processing in all sectors except the public sector, it is useful to also examine its definition of personal information. The draft law on data protection in Nigeria defines personal information as '… information about an *identifiable individual*, but does not include the name, title or business address or telephone number of an employee of an organisation.'[68] It is unclear why the latter part of the definition '…but does not include the name, title or business address or telephone number of an employee of an organisation' was included or the purpose it was intended to serve. This is more so since it is being proposed to remove the

[66] s 1 NCC SIM Registratration Regulations, 2011.
[67] ibid.
[68] s 33(1) Personal Information and Data Protection Bill 2013 (emphasis added).

same clause from the PIPEDA which the draft law models.[69] The only explanation therefore is that the draft law included the provision simply because the PIPEDA is phrased in similar terms.[70] Notwithstanding the exclusion however, it appears that the definition of personal information under the draft law is broader. For example, legislative and judicial authorities in jurisdictions like the UK and Canada suggest that the correct interpretation of "identifiable individual" is crucial to defining the categories and scope of personal information. It is necessary to turn to these authorities to determine the meaning and scope of 'information about an "identifiable individual".

5.3.1.1 Understanding the Meaning of Personal information from a Comparative Perspective

According to the Canadian Supreme Court, the intent of the law in using the term "identifiable individual" '… is to capture *any information* about a specific person…'[71] Also, according to the Canadian Federal Privacy Commissioner, personal information includes any information that has even the smallest potential of being about an identifiable individual.[72] Critiquing this position, one commentary noted that this approach justifies the classification of all sorts of information as personal irrespective of whether or not the information is sensitive, private, innocuous or well-known.[73] In effect, under the PIPEDA, *any information* is personal information.

A similar approach to the above was taken by the EU Article 29 Working Party on Data Protection (hereinafter WP29) in construing the notion of identifiability under EU law.[74] The EU Directive on Data Protection defines personal data as follows:

> …any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or

---

[69] see Bill C-12: An Act to Amend the Personal Information Protection and Electronic Documents Act 19 October 2011.
[70] see PIPEDA 2000, s 2(1).
[71] *Dagg v Canada* (Minister of Finance) [1997] 2 S.C.R 403, 405.
[72] See Federal Privacy Commissioner of Canada, 'Annual Report to Parliament 2001-2002' 56 <https://www.priv.gc.ca/information/ar/02_04_10_e.pdf> accessed 12/01/2014.
[73] See Kris Klein, 'Canadian Privacy Data Protection Law and Policy for the Practitioner (2012) International Association of Privacy Professionals (IAPP) Publication, 13.
[74] The provisions of the EU Directive are preferred here because EU law is the reference standard even for UK data protection law. Also, since reforms to the EU Data Protection Law propose a regulation rather than a directive, it is anticipated that the UK law will eventually be in complete harmonisation with EU law.

> more factors specific to his physical, physiological, mental, economic, cultural or social identity.[75]

According to the WP29, the significance of the definition lay in the fact that it is sufficiently broad to cover *all* information which may be linked to an individual and instances where personal data might be at risk.[76] Therefore, although the EU law provides specific examples from which inferences may be drawn that information is personal, that is, factors specific to a person's physical, physiological, mental, economic, cultural or social identity, its position is not different to that taken by the Canadian authorities. This is particularly so since the WP29 Opinion further noted that in order to determine whether a person is identifiable, recourse must be taken to Recital 26 of the Directive. The Recital provides that in order to determine whether a person is identifiable, "account should be taken of all the means likely reasonably to be used … to identify the said person."[77] In this respect, the WP29 asserts that all forms of information qualify as personal data unless the possibility of identification does not exist or is negligible.[78] Personal data therefore includes factual identifiers such as a person's name, address, date of birth, and indirect identifiers such as phone numbers. It also includes profile data drawn from a combination of innocuous information,[79] and information relating to devices and objects such as IP addresses,[80] web traffic surveillance tools including cookies, and geolocation and traffic data.[81] The WP29 further indicated that prospective or merely speculative data can be personal information when it noted that consideration must be given to the state of art in technology because information which is currently unidentifiable may subsequently become identifiable due to technological development.[82]

The above implies that under EU law, identifiable information could also be any form of information. Correspondingly, an individual is identifiable, if there is a possibility of

---

[75] See Directive 95/46/EC, art 2(a).
[76] Article 29 Working Party, *Opinion 4/2007 on the Concept of Personal Data* (WP 136 20 June 2007) 4-5.
[77] Directive 95/46/EC, recital 26.
[78] Article 29 Working Party (n 76) 15.
[79] ibid 14.
[80] ibid; see also Article 29 Working Party, Privacy on the Internet – An Integrated EU Approach to On-line Data Protection (WP 37 21 November 2000) 21.
[81] Article 29 Working Party, *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices* (WP 185 16 May 2011); see also Proposal for a Regulation of the European Parliament and Council COM (2012) 11 final, art 4(1), (2) (hereinafter General Data Protection Regulations)
[82] Article 29 Working Party, *Opinion 4/2007 on the Concept of Personal Data* (n 76) 15.

identification even if identification is yet to occur. In effect, the scope of potentially identifiable information is indeterminable and likely to constantly change in the technological context. This approach to defining personal information is essentially expansionist and is regarded as fundamental to protection particularly in view of developing technologies.[83] It is therefore possible to argue that if the interpretation of "identifiable individual" in the Nigerian draft law follows either the Canadian or EU approach, the result would be a broad and all inclusive definition of personal information. The crucial question is whether this is the correct approach to interpretation. In other words, should there be a threshold definition for personal information and what should the threshold be? The following sections provide an answer by examining both the expansionist approach and alternative proposals for definition of personal information.

(a) Personal information is all Information - Why not the Expansionist Approach?

The objective of the expansionist approach to defining personal information is to protect not only information considered personal already but also those which may become potentially so. Its main advantage is flexibility which implies that new forms of personal information created by new technologies could fall within its ambit. However, flexibility also means the definition of personal information is open-ended, unstable and ambulatory. For example, with the evolution of the 'internet of things', arguments now surround the legal treatment of physical (even household) objects and the extent to which they might constitute personal information. [84] Therefore, with developments in identification technologies including re-identification techniques, data mining, profiling and the use of big data as well as ubiquity brought about by cloud computing, almost any data can now be personal.[85] While the expansionist approach promotes flexibility therefore, the flip side of the coin is that it can also produce speculations and uncertainty.

For example, additional consequences of adopting the expansionist approach include increased administrative and compliance costs. These arise because organisations have to protect information that is potentially but not actually identifiable. On the part of regulators, additional cost is incurred to ensure compliance. Citing in particular information processed

---

[83] ibid 4.

[84] See Douwe Korff, 'Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments' (2010) EU Working Paper No 2, 49.

[85] see eg Article 29 Working Party, *Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with regard to the Processing of their Personal Data in the EU* (WP 221 16 September 2014).

by cloud service providers, Korff argues that enforcement authorities may have difficulties establishing control over such data processing because the cloud service provider is located in a foreign jurisdiction.[86] Therefore from the perspectives of enforcing the law, a broad definition of personal data will entail increased administrative costs not only because it requires protection for almost all data, but also because in spite of the costs, certain organisations cannot be compelled to comply with the law. More crucially, the expansionist approach appears to equate privacy protection with data protection. For example, an all-inclusive definition of personal information creates a real risk of bringing all information under the rubric of 'personal'. On this point, Robinson et al argue that enforcement and regulation of EU law is undermined by the strong links between privacy and data protection.[87] This observation is particularly relevant to Nigeria where both the notions of data protection and privacy are relatively nascent and likely to be conflated.

The empirical data collected in the process of this research suggests that service provider organisations in the Nigerian e-payment industry already assume that protecting personal data also equals protecting the general privacy rights of users. As noted by some providers, users generally exhibit bad privacy behaviour and choices. Users for example fail or are incapable of changing default PINs, passwords, and other access codes.[88] They also tend to share personal (financial) information with friends, family and at times even with strangers.[89] This behaviour, it was argued, points both to failure to appreciate the nature of threats in electronic transactions and a cultural bias towards disregarding certain information as private. The conclusion therefore is that under a data protection regime, the problem will not be so much that service providers fail to protect personal information but that users' behaviour is inconsistent with imposing data protection obligations on the providers.

Citing examples of alleged bad privacy behaviour, a service provider noted that his organisation has at various times monitored users on its ATM machines. Such observations reveal that users would often disclose their PINs to complete strangers particularly when they are struggling to remember the PINs. In his view, 'If they [the customers] could trust complete strangers and allow them [the strangers] to handle their cards and help change or

---

[86] Douwe Korff, 'The Use of the Internet & Related Services, Private Life & Data Protection: Trends & Technologies, Threats & Implications' (Council of Europe T-PD 2013) 07.
[87] Neil Robinson et al, 'Review of the European Data Protection Directive' (Rand 2009) 14. <http://www.rand.org/pubs/technical_reports/TR710.html>accessed 13/05/2014.
[88] Payment Service Provider 4.
[89] Payment Service provider 8.

remember their PINs, we can assume they do the same with friends and family.'[90] Another service provider stated that his organisation was also aware that users often solicit the assistance of complete strangers either to activate their accounts or to change or input their PINs (mostly on ATMs). As he noted, if people do this on ATMs which is relatively easier to use, one can envisage what they will do when it comes to using the internet. His view is that the internet is more complicated to use and less accessible than the ATM. Therefore users are likely to give out even more damaging details such as card numbers, CVV, card expiry date and so on just to have others help them initiate or complete transactions online.[91]

Another example which appears to validate the fears of the providers relates to where a seeming customer had attempted to retrieve a payment card which had been withheld by the bank's ATM because of incorrect PIN inputs. As the service provider noted, having completed the necessary forms needed to establish the customer's identity and satisfied that the information provided matched those in the records of the bank, the 'customer' was asked to provide his signature. However, as the provider noted, '… very curiously, he [the customer] could not provide a matching signature'.[92] Upon the threat of arrest, the 'customer' admitted that the card belonged to his twin. According to the provider;

> [To] prove to us that he had authority to use the card, right before us, he called three other people who are privy to the account. His brother, whom he could not reach, his brother's wife, who confirmed she also knew the PIN but could not remember, his own wife, who also did not remember the PIN. You do have to ask how long this chain of trust should be, because it just goes on.[93]

The above examples indicate that organisations already anticipate a regulatory breach or failure based on their inability to regulate the behaviour of users. However, it can be argued that this assumption is based on the lack of understanding between individual privacy rights and behaviour and obligations which may be placed on organisations to regulate data processing. It may also be argued that users' privacy behaviour referred to by service providers merely reflect cultural perceptions of privacy which, in the African context is essentially communitarian rather than intuitionist.[94] In effect, rather than representing a

---

[90] ibid.
[91] Payment service provider 4.
[92] Payment service provider 6.
[93] ibid.
[94] Alex Boniface Makulilo, 'Data Protection Regimes in Africa: Too Far from the European 'Adequacy Standard?' (2013) 3(1) International Data Privacy Law 42.

lack of desire for privacy, users' behaviour may demonstrate the implicit de-emphasising of the notion of individualism in association with privacy in the African context. This notion is neither correct nor incorrect as cultures and individuals tend to define privacy differently.[95] Although, literature is sparse on the notion of privacy in the African context, generally, it is conceived that Africans have less understanding of and little use for privacy. According to Gutwick, the fact that the African Charter on Human and People's Rights omits a right to privacy is a vindication of this position.[96] In his 2007 thesis on 'The right to Privacy in Nigeria', Nwauche contends this position. He asserts that the conclusion that Nigerians are not in need of privacy is based on a superficial assessment of our situation and circumstances.[97] While his implicit argument was that people need and value privacy, he supports the view only by reference to the constitutional right to privacy rather than by specific evidence of how the need or value for privacy manifests in the Nigerian society.[98] Makulilo's exposition of the African literature on privacy however suggests that the African culture of communism may be responsible for this perception. As he argues;

> The main thrust of the literature is that privacy in Africa is undeveloped because of the prevalence of the culture of collectivism as opposed to the Western culture of individualism. Accordingly,…as Africans live in associations, an individual is denied a space for claiming his/her right to privacy.[99]

Also in their analysis of the South African culture of *ubuntu* and its relationship with privacy, Olinger, Britz and Olivier, describe the African view of privacy as one founded on communism rather than individualism. According to the authors, ethical decisions are made based on the worldview that the group or community interests supersede that of the individual. Privacy is therefore secondary to relationship building and concepts such as

---

[95] Lee A Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) Stockholm Institute for Scandinavian Law 166; see also Subhajit Basu, 'Privacy Protection: A Tale of Two Cultures' (2012) 6(1) Masaryk University Journal of Law and Technology 1.
[96] S Gutwirth, 'Privacy and the Information Age' cited in Alex Boniface Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163, 168.
[97] E.S Nwauche, 'The Right to Privacy in Nigeria' (2007) 1(1) CALS Review of Nigerian Law and Practice 64.
[98] ibid.
[99] Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (n 96) 163.

protection of personal information are bound to be interpreted as secrecy rather than protection in the context of such societies.[100]

In context, rather than interpret the above cited user behaviours as lack of desire for privacy, they are better understood as a different articulation of privacy interests, values and priorities. As Bygrave argues, since concerns for privacy are uneven across cultures and jurisdictions, the fact that many African countries lack comprehensive privacy protection regimes is not to be taken as symptomatic of a propensity in African cultures to place primary value of securing the interests and loyalties of the group at the expense of the individual. He concludes that care must be taken not to paint countries and cultures into static categories.[101] As Basu also rightly asserts;

> …the existence of multiple cultures and philosophies prompts questions regarding the appropriateness of hegemonic relations and the privileging of one culture over another. The question is whether privacy is deemed inherently valuable by all people or whether its value is relative to cultural differences.[102]

In addition to cultural specificity, it is also possible to argue that privacy is individually relative. Therefore, as far as privacy goes, one could contend that a person has the right to deal with his personal information however he likes. Judicial authority and the literature support this point. To underscore this subjective notion of privacy, the Supreme Court of Nigeria upheld a plaintiff's right to refuse medical treatment, a decision which ultimately led to her death. According to the court, as long as there are no overriding state interests, the recognition of a person's right to privacy also entails his right to be left alone to choose any course of life.[103] Concomitantly, it can be argued that in the absence of a legal or moral duty to protect one's personal information, one may disclose personal information to anyone of one's choice including friends and family. Furthermore, because rights and duties are correlative and inclusive, it is also possible to argue that it is infact impossible to owe such a duty

---

[100] H.N Olinger, J.J Britz, M.S Olivier, 'Western Cultures and Ubuntu- Influences in the Forthcoming Data Privacy Bill' <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.3533>accessed 03/01/2014.

[101] Bygrave, (n 95) 176.

[102] Basu, (n 95) 15.

[103] See *Medical and Dental Practitioners Disciplinary Tribunal v Dr John Emewulu Nicholas Okonkwo* (2001) 7 NWLR Pt 711, 206, 244 para E.

to oneself as this will also imply that one has a claim or right against himself. Many years ago, Singer instructively observed as follows:

> But it follows from this that to have a *duty to oneself* would be to have a right against oneself, and this is surely nonsense. What could it mean to have a right or a claim against oneself? (Could one sue oneself in a court of law for return of the money one owes oneself?)[104]

In other words, it is to be presumed that it within a person's right to violate or invade his own privacy.[105] As legislative and judicial authorities establish, what the law seeks to protect is when access is unwanted or unwarranted, or where it is criminal. This position is supported by Westin's classic definition of privacy as 'the claim of individuals …to determine for themselves when, how and to what extent information about them is communicated to others'. [106]

The objectives of data protection laws were discussed earlier in this chapter. It was noted that the laws emphasise rules to be applied by organisations when processing data. It is therefore not so much about a person's right not to disclose personal information but about organisations' duty of management and security. However, while the foregoing arguments suggest that organisations' assumptions about the objective of a data protection law and how it affects individual's rights of privacy are incorrect, they nevertheless underline the existing biases and perceptions on data protection. It may therefore be correct to argue that a vague and overly broad definition of personal information promoted in the expansionist approach could aggravate the problems. It would make the determination of personal information ad hoc and infinite and thus create uncertainty for organisations and regulators. This position is correct in spite of the advantages of the expansionist approach in the area of incorporating new technologies. Regarding similar concerns about the scope of personally identifiable Information (PII) in the US, [107] Ohms correctly argues as follows:

> No matter how effectively regulators follow the latest reidentification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of

---

[104] Marcus G Singer, 'On Duties to Oneself' (1959) 69(3) Ethics, 202.
[105] Compare arguments by Allen, see Anita L Allen, 'An Ethical Duty to Protect One's own Information Privacy' (2014) 64(4) Alabama Law Review 845.
[106] Alan F. Westin, *Privacy and Freedom* (Ătheneum, New York 1967) 7.
[107] The PII is the American equivalent of the European concept of personal data.

> potential PII [personally identifiable information] will never stop growing until it includes everything.[108]

Therefore, if we argue that data protection law is not equal to the protection of the general right of privacy, it is only logical that we be clear about what data protection law protects. The arguments below examine alternative approaches to defining personal information and their utility in contrast to the expansionist approach.

(b) Risk of Harm based Approach to Defining Personal Information

The risk of harm based approach determines whether information is personal depending on whether its use could cause harm. Two approaches appear to have been advocated here. The first defines personal information progressively based on a multi-stage or multi–level assessment of the risk of harm. The second proposes that information be defined as personal only when the risk of harm is objectively assessed rather than subjectively determined.

i. Risk of Harm as a Multi-stage Process

Following the first approach, Hon, Millard and Walden suggest that given the complex technology environment, a two-stage technologically-neutral, accountability-based approach to address privacy concerns in the context of personal data protection should be adopted.[109] The first stage is based on a risk of identification. At this stage, it is proposed that appropriate technical and organisational measures should be taken to minimise the risk of identification. It is therefore only if the resulting risk remains sufficiently high that data should be considered personal. The second stage proceeds to assess the risk of harm identified in the first stage and its likely severity. If sufficiently severe, appropriate measures must be taken, regarding the personal data, with obligations being proportionate to risks.[110]

Similarly, Schwartz and Solove's reconceptualization of the concept of PII proposes a risk of harm based approach dependent on whether information is identified or identifiable. They argue that the problem with the expansionist approach is that it creates a continuum of risk which equates identified information with identifiable information. To break the

---

[108] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation' (2010) 57 UCLA Law Review 1701, 1742.
[109] W Kuan Hon, Christopher Millard and Ian Walden, 'The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated? – The Cloud of the Unknowing' (2011) 1(4) International Data Privacy Law 211, 214-222.
[110] ibid 227-228.

continuum, the authors suggested differential application of standards of fair information practices (FIPs) (or data protection principles). In this respect, they identified three categories of personal information as identified, identifiable and non-identifiable information. Schwartz and Solove further proposed that for identified personal data, all FIPs should apply, because this data already relates to a known individual and carries a higher risk of harm. For identifiable information, only the core principles of FIPs particularly data quality, data security and transparency should apply.[111] This is because identifiable information is yet to relate to a specific individual and may never do so. No FIPs should apply to non-identifiable information because they are not relatable to any person taking into account all means likely to be used for identification.[112]

The above proposals are persuasive but are generally complex. They are persuasive because in contrast to the disconnected notion of identifiability adopted by the draft law and promoted in the expansionist approach, they take cognisance of real risk of identification as well as the notion and possibility of harm resulting from the identification process. The complexity however derives from the multi-stage or multi-level assessment and application proposed by the authors. For example Schwartz and Solove propose a model which means information which was at first unidentifiable may later become identifiable. Once identifiable, the information triggers the application of all FIPs.[113] This makes it difficult to see how the scope of the concept can be narrowed even by reconceptualising personal information. Arguably, it simply produces a circular process where unidentifiable information becomes identifiable at some point in time. This in turn produces uncertainty around personal information similar to the expansionist approach. The same argument applies to the proposal made by Hon et al to first minimise identification and then apply data processing rules proportionate to the risk. One can argue for instance that developments in re-identification and aggregation technologies suggest that even when data is de-identified, a subject could subsequently become identifiable or identified.[114] In both proposals, the application of data processing rules proportionate to the risks results in different levels of protection for personal information. Indeed, Schwartz and Solove admit that at its best, their approach produces different levels of safeguard for

---

[111] Paul M. Schwartz and Daniel J. Solove, 'The PII problem: Privacy and a new concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814, 1881.
[112] ibid 1880-1887.
[113] ibid 1879.
[114] see eg Article 29 Working Party, *Statement of the WP29 on the Impact of the Development of Big Data* (n 85).

different categories of data.[115] Significantly therefore, for nascent data processing regulatory environments like Nigeria, the proposal may be complex to apply. For example, since the proposal will translate into applying different rules to different categories of personal information and even to the organisations processing the data, it can also create confusion and inconsistencies in the application of data processing principles.

ii. Objective Risk of Harm –The Purposive approach

Gratton,[116] Cate[117] and Calo[118]offer alternative views based on the identification of an objective risk of harm. Similar to Millard and Walden, the authors argue that to establish that information is personal, it is useful to query the nature of harmful consequences arising from the use of such information. They however go further to suggest that it is equally important to determine whether such harmful consequences are the focus of data protection laws. In this respect, Calo distinguished between subjective and objective privacy harms. He conceived subjective privacy harm as unwanted perception of observation. Subjective harm denotes the degree of antipathy which an individual feels towards being observed and may result in mental, emotional or psychological distress. This harm is subjective in the sense that it is internal to the person being harmed.[119] According to Calo, the key requirement in subjective privacy harm is that observation is unwanted. To demonstrate this, he argues that when a person himself publicises personal information or understands and agrees to its use, he does not invoke the sense of violation or harm. However, a person feels violated if the same information was collected by surreptitious means.[120] Conversely, Calo argues that objective privacy harm is the unanticipated or coerced use of information concerning a person against that person. To constitute objective privacy harm, information use must be unanticipated.[121] Objective categories of privacy harm are therefore negative and external actions justified by reference to personal information. Examples include the unanticipated sale of a user's information that results in spam, or exploitation for crimes such as identity theft.[122] Cate correctly associates the

---

[115] Schwartz and Solove, (n 111) 1877.
[116] Eloise Gratton, 'If Personal Information is Privacy Gatekeeper, then Risk of Harm is the Key: A Proposed Method for determining what Counts as Personal Information (2013) 24(1) Albany Law Journal of Science and Technology 1.
[117] Fred H Cate, 'The Failure of Fair Information Practice Principles' (2006) <http://ssrn.com/abstract=1156972> accessed 05/10/2014.
[118] Ryan Calo, 'The Boundaries of Privacy Harm' (2011) 86(1) Indiana Law Journal 1.
[119] ibid 15.
[120] ibid 23.
[121] ibid.
[122]ibid 4 -15.

harmful consequences here not with the concept of individual control but with the need to protect individuals from uses of information which are unfair or harmful in a tangible or objective way.[123]

Following a similar track, Gratton argues that the categorisation of information as personal must coincide with the ultimate purpose of data protection laws. As she observes, the legislative intent behind data protection laws is protecting the privacy of individuals from harmful consequences which may arise from organisational processing of personal information. This is the purposive rule of interpretation, which examines the aims of the drafters of a law and the objective underlying the legislation. Therefore, particular types of data handling activities must carry an underlying risk of harm which is objective rather than subjective.[124] As Gratton, argues, being under surveillance or dignitary harm are examples of harm which could fall under the subjective category.[125] However, harms including financial, economic or physical harm other than distress would be objective harms which are the proper concerns of data protection legislation. As an example therefore, if financial information is released by or stolen from banks, it can lead to objective harms such as fraud or identity theft.[126] As a further example therefore, it can be argued that while opinions may differ on how people feel about being monitored by closed circuit television (CCTV), virtually everyone would be apprehensive of possible uses of their information if their bank was hacked.

Based on the foregoing arguments, it would be correct to argue that the 'objective risks of harm' test provide some guidance on how best to approach the notion of identifiability and the concept of personal information in Nigeria. For example considering the characteristics of subjective risk of harm discussed above, and nature of information gathering and collection, it is arguable whether the objective of data protection laws is protection from such harms. It was noted earlier that for the purpose of the law, the question is not whether information can be collected, invariably they can, whether contractually or surreptitiously, therefore data protection laws do not prohibit information collection. By logical extension, it can be argued, that the law should not also focus on the subjective risk of harm associated with such collection. Therefore, the definition of personal information would depend on what use or processing could cause harm rather than what uses a person merely finds inconvenient or simply dislikes.

---

[123] Cate, (n 117).
[124] Gratton, (n 116) 45.
[125] ibid 47.
[126] ibid 68.

Moreover, even if one does not agree that the above is the objective of all data protection laws, it could be helpful to look at objectives from the points of views of respective jurisdictions. Along these lines, it can be argued that the definition of personal data in the EU is more aligned to protecting 'dignitary privacy',[127] hence its focus on all and any information. In contrast, other laws lay emphasis on the prevention of commercial exploitation of privacy.[128] The APEC framework focuses on preventing harm to individuals from the wrongful collection and misuse of their information and even incorporates a 'preventing harm' principle.[129] Although the draft data protection law in Nigeria models the PIPEDA, the objectives differ. One of the objectives of the PIPEDA is to meet the adequacy requirement under EU law. In contrast, one of the main motivations behind the Nigerian draft law on data protection is the prevention and control of identity related crimes. According to the Nigerian Attorney General, the bill is '… a demonstration of the government in its resolve towards providing assured and sustainable identity infrastructure … [which] will in turn give the populace a decent robust and crime free environment.'[130]

Therefore, because the jurisprudence of privacy is arguably not well understood and enshrined in Nigeria, the (objective) risk of harm based approach helps to avoid the conflation and dilution between the concepts of data protection and privacy. It was noted above that organisations' perceptions of data protection tends to be that a law would be ineffective because of users' behaviour towards protecting their (users) privacy. From these perspectives, less focus on broader privacy rights will encourage compliance because organisations do not see themselves as mere custodians of abstract privacy interests but as having a purpose, that of preventing (objective) harm which may result from misuse or misappropriation of personal information. The objective risk of harm approach is therefore useful both in setting the threshold for identification and in the area of enforcement and compliance.

A final point which needs to be mentioned, in particular as it relates to determination of personal information in financial transactions such as e-payments, is the risk of under-inclusiveness. Based on the risk of harm approach above, it can be argued that potentially

---

[127] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005) University of Ottawa Law and Technology Journal 357, 388-389.
[128] See eg Preamble to APEC Privacy Framework 2005.
[129] ibid Principle 1.
[130] 'Adoke lauds NIMC over bill' <http://citizensplatform.net/2013/02/adoke-lauds-nimc-over-bill/>accessed 17/01/2104.

identifiable (financial) data may be left out because even objective harm can be relative to specific processing activities or information. A way out however is to consider an exposition of identifiability developed around the concept of contextual harms. For example, we may ask, what the possibilities are that IP addresses can lead to identification much less to financial harm in e-payment systems. As noted by one commentary;

> [T]he nature of IP addresses means that an address can either be dynamic or static, and in most cases addresses tend to be dynamic. This means that each time an individual makes an online connection, the IP address would be different from the one they used the last time they went online.[131]

If this observation is correct and if things have digital identities as noted in the discussion of identities in chapter three, then the appropriation of the identity of things to individuals is confusing and needless. Ultimately, the correct interpretation of the notion of 'identifiability' and the definition of personal information in Nigeria must rest on the answers to three main questions. These are; what is the purpose of the data protection law? What is the nature of the harm it proposes to address? Do these harms fit into the niche area of data protection or are they better addressed by broader privacy legislation?

5.4 Challenges of Enactment, Administration and Enforcement of Data Protection Law

The foregoing arguments show the relevance of data protection law to the protection of personal information particularly when held in proprietary databases. The analysis underlined the need for a general legislation which would address the crucial issue of the scope of personal information and include a comprehensive set of data protection principles. However, unlike the cybercrime law, proposals for data protection have been relatively sparse. The draft bill 2013 appeared to be the first comprehensive bill on data protection.[132] The empirical data suggests that similar to the cybercrime law, there are institutional and systemic factors which impede the passage of a data protection law and which may affect its effectiveness. These include institutional lobby, the pervasive culture of compliance and identity management problems.

---

[131] Ministry of Justice, 'Summary of Responses Calling for Evidence on Proposed Data Protection Legislative ital-communications/data-protection-proposals-cfe/results/summary-responses-pFramework' (28 June 2012) 12 <https://consult.justice.gov.uk/digroposed-data-protection-legislation.pdf>accessed 23/05//2014.

[132] It is more usual to find data protection requirements inserted as small sections within cybercrime laws. See eg s 21 Cybercrime Bill 2014.

5.4.1 Institutional lobby against legislating on data protection

The data suggests the existence of lobby interests for and against regulation of data processing in Nigeria. On the one hand, and in addition to service providers' perceptions of the role and limits of data protection law highlighted above, service provider organisations and their regulators also appear to view data protection requirements in any new legislation as burdensome and over-regulation.[133] According to one regulator, because of differences in industry practices, industry regulators can more effectively oversee issues relating to data protection and already do.[134] Payment service providers themselves cite compliance with the bankers' duty of secrecy as the basis of 'effective' data processing practices. In other words, the contention here is that a general law is not required for data protection in Nigeria. On the other hand, some stakeholders query the existence or adequacy of any industry regulatory initiatives in the area of data protection. A policymaker observed for example that whatever rules the telecoms and banking industry claim to apply to data processing must be known only to the industry. He argued that consumers are seldom aware of such rules much less be able to enforce them. The policymaker concluded that the very idea that industry is regulating itself is suspect and more transparency is needed if indeed data protection rules exist.[135]

It is arguable that the above observations in themselves cannot be taken as representative of the position of all sectors and industry processing data. However, further inferences of the existence of lobby interests can be drawn from the provisions of the draft law on enforcement. For example, although the law proposes the establishment of the office of the privacy commissioner who will be a public officer, the powers of the commissioner are minimal. The functions of the commissioner include monitoring and supervising compliance with the provisions of the law.[136] Specifically, the Commissioner is empowered to carry out inspection of personal data and information systems.[137] As part of the remedial procedures under the draft law, the Commissioner may receive complaints from individuals alleging organisations' contravention of the law or may independently initiate investigations where there are reasonable grounds for doing so [138] The independence of the Commissioner is guaranteed by provisions of the draft law which provides that the commissioner shall be

---

[133] Payment Service Providers 7, 8.
[134] Regulator 1.
[135] Policymaker 3.
[136] s 4 (4) (a) Cybercrime Bill 2014.
[137] ibid s 4 (4) (e).
[138] ibid s 10 (1), (2).

immune from civil or criminal prosecutions for activities carried out in good faith during the conduct of his duties.[139] The Commissioner is also only accountable to the National Assembly to which he is required to render annual reports concerning the activities of his office on the application of the Act.[140]

The above provisions of the law indicate that a notable aspect of the provisions is the independence and apparent powers of the privacy commissioner. However, these powers are neither specific nor adequate. For example, the Commissioner has no enforcement powers such as the powers to impose fines or penalties, or even to make orders directing organisations to cease specific activities. The law itself omitted the creation of any offence and failed to prescribe penalties for infractions or contraventions of the law.[141] Corresponding to the threats to personal information from data breaches, the Commissioner does not also have the power to require mandatory reports of data breaches or to receive such reports. The provisions can be contrasted with those under EU law.[142] For example, the UK Data protection Act (DPA) vests the Information Commissioner's Office (ICO) with more extensive administrative and enforcement powers.[143] Also, unlike the draft law, the DPA creates a number of offences and penalties. Unlawful obtaining of personal data whether knowingly, recklessly and without the consent of the data controller is an offence.[144] It is an offence to unlawfully obtain or to sell personal data.[145] Offers to sell or advertisement indicating that personal data is for sale is also an offence.[146] Processing of personal data without notification to the Information Commissioner, or failure to comply with enforcement notices are further offences under the Act.[147] Offences are generally punishable with fines, and to address the perceived ineffectiveness of fines as deterrence to contraventions of the law, proposals were made for the imposition of custodian sentences, in particular for the DPA section 55 offences.[148]

The law further empowers the ICO to impose large monetary penalties (up to £500,000) for serious breaches of the Data Protection Act. The ICO may also institute criminal

---

[139] ibid s 23(1), (2).
[140] ibid s 27(1)-(3).
[141] ibid ss 14, 15, 16, 17(a)-(c).
[142] See Directive 95/46/EC, recital 62.
[143] See Data Protection Act 1998, s 40.
[144] ibid s 55(1).
[145] ibid.
[146] ibid ss 55(4), (5), (6).
[147] ibid s 47.
[148] ibid s 55A-55E; see also Justice Committee, *The Functions, Powers and Resources of the Information Commissioner* (HC 2012-13 962) 13-17.

proceedings against a person who has committed an offence under the Act and a person found guilty of an offence may be subject to a fine up to £5,000 in the Magistrates' Court and unlimited fines in the Crown Court. Under the proposed reform to the EU law, breach notification and reporting to the ICO will be mandatory, and enforcement powers would be further expanded through the establishment of the European Data Protection Board (EDPB).[149] In view of the propensity of organisations to undermine regulation through non-compliance discussed below, it is arguable that enforcement powers similar to that of the UK ICO's are a prerequisite to the effectiveness of the proposed data protection law in Nigeria.

Based on the foregoing, it seems safe to assume that the weak approach to administration proposed in the draft law represents a form of compromise between those proposing soft law and hard law approaches to data protection. In effect, the fact that a law is proposed at all is likely to appeal to policymakers and other stakeholders canvassing for a general law. Conversely, by watering down the regulatory powers, the law will also arguably be acceptable to service providers/organisations with inclination for soft law or industry regulation. Invariably, inadequate enforcement powers will simply create a situation of a "bad law is better no law" which would not significantly improve the status quo. Nevertheless, the critical point here is that the position taken by the law appears to support the existence of institutional lobby against a data protection law.

5.4.2 Non-compliance with Regulation- 'The Culture of Impunity'

Besides the challenges of lobby groups, the empirical data also suggests that implementing data protection law in Nigeria may be affected by the pervasive culture of non-compliance with law and regulations. According to a lawmaker and a policy maker for example, notwithstanding the breadth of legislation, regulation of data protection would fail because of the pervasive 'culture of impunity' in Nigeria.[150] It is instructive to mention that this means non-compliance is a systemic problem rather than a peculiarity of any regulatory regime. Generally, the culture of impunity is characterised by disregard for the rule of law including disobedience of regulatory and court orders without fear of reprisals or punishment. Accordingly, the OECD defines systemic failure of compliance as widespread and durable non-compliance characterised by failures of public governance that devalue

[149] See General Data Protection Regulation, arts 31-32.
[150] Lawmaker 3, Policymaker 2.

regulatory instruments.[151] Ultimately, systemic non-compliance breaks down the credibility of government and governance under the rule of law, and creates unnecessary costs through fruitless administration and implementation.[152] It also leads to the postponement of the achievement of policy objectives and erodes confidence in the use of the regulation, the rule of law, and government in general. The cumulative effect of non-compliance is to undermine the efficacy of any legal or regulatory instrument.[153]

As noted above, non-compliance is a systemic problem of regulatory mechanisms in Nigeria. However, it is possible to argue that these are generally aided by ineffective regulatory oversight. The implications of lack of enforcement powers discussed above support this view. In addition, and in the particular context of the draft data protection law, perceptions that regulation is unfair may also exacerbate the problems of non-compliance. To illustrate, it was noted in chapter three that personal information used for identity related fraud need not be obtained exclusively from financial institutions' databases. They can be obtained from different databases including non-financial and government owned databases.[154] In recognition of this threat, data protection laws often require compliance with data protection principles by both public and private sector organisations.[155] This is arguably good law and good practice. However, under the draft law on data protection in Nigeria, government institutions' are exempted from the operation of the law. The draft law provides quite unequivocally that 'This Act does not apply to any government institution.'[156]

There are two possible bases for this exemption. The first is that similar to the Canadian PIPEDA which it copies, the draft law exempts government institutions because they are already regulated by other legislation. Even if this explanation is correct, it would still mean data processing by public institutions remain largely unregulated. As noted earlier in this chapter, the Freedom of Information Act is inadequate regarding public sector data processing.[157] The alternative explanation is that the law is a reflection of the lack of political will to subject government and its institutions to regulation and accountability.

---

[151] See OECD, 'Reducing the Risk of Failure: Challenges for Regulatory Compliance' (2000) 10<http://www.oecd.org/gov/regulatory-policy/46466287.pdf> accessed 11/11/2014.
[152] ibid.
[153] ibid 13.
[154] See notes in 3.3.2.1 Hacking (Unauthorised/Illegal Access to computer Systems) p 56 at 59.
[155] See eg definition of data and data controller under the Data Protection Act 1998 Act s 1.
[156] s 2(2)(a) Personal Information and Data Protection Bill 2013.
[157] See notes above at p 145.

This explanation is particularly persuasive. For example, the draft law was proposed by the Nigeria Identity Management Commission (NIMC), a government institution, however, the same law proposes to exempt government institutions, ostensibly including the NIMC itself, from its operation.

On both legal and ethical grounds, the exemption of government institutions may seem unfair to private organisations that would be required to comply with the law. On ethical grounds, it could be deemed unfair for the law to exempt the NIMC, which has the potential to be the largest collector of personal information in Nigeria, while subjecting smaller organisations to regulation.[158] According to research, if people feel they are treated unfairly by the government or a regulatory agency, they will often respond by refusing to comply with regulatory requirements. Conversely, people who believe they have been or will be dealt with fairly by a regulatory system are more likely to comply with its requirements, whatever they are.[159] The exemption of government organisations may therefore underline unequal power relations which may promote perceptions of oppression.

On legal grounds, the exemption suggests inequity in the application of the law which may have consequences for the liability structure in the payment industry. For example, payment service provider organisations may justifiably argue that data breaches originate from government organisations that also collect personal information but without observing the principles of data protection. This may lead to shifting liability for fraud towards such organisations which could then escape any liability on grounds that they are not subject to law.

It is important to mention that the above is not intended to undermine the attendant problems of non-compliance with regulatory regimes in Nigeria but simply to underline the factors which promote non-compliance. In the particular context of the draft data protection law, the creation of different standards for private and public organisations means the law itself invariably promotes non-compliance.

5.4.3 Challenges of Identity Management

Lack of credible identity management systems is perhaps the most significant basis for questioning the enforceability of a data protection regime in Nigeria. To underline the importance of identity management to data protection, one respondent explained it by

---

[158] See notes above at p 137.
[159] See OECD, 'Reducing the Risk of Failure: Challenges for Regulatory Compliance' (n 151) 19.

analogy derived from local folklore.[160] According to the story, a village elder once had a calabash[161] which he had engraved for identification and distinction. The calabash was later stolen or misplaced. Unperturbed, the elder boasted to his friends that he would readily find the calabash because he had a mark on it. One of his friends however pointed out that this logic was defective and the reverse was actually the case. In effect, until he (the village elder) finds the calabash, he cannot find the mark on it. The allegory is often captured by the saying, *'igba sonu, o ni o sami si, sebi ti o ba ri igba ni o ma ri amin'*. Literally this translates, 'the calabash is lost and you boast that you have an identifying mark on it, is it not when you find the calabash that you will find the mark?' The moral is quite straightforward, that is, unless there is an independent means of finding the calabash, insisting on the mark as an identifier is illusory.

Translated into identity management and data protection contexts, the above analogy means that merely having a data protection law provides scant protection unless the law is also supported by credible identity management systems. Stated simply, there is misplaced confidence in the identification process, which means that authentication becomes problematic. Identity management is crucial in two aspects here. One, it helps to establish that individuals are who they say they are. Two, it ensures that criminals who use stolen identities can themselves be identified as fraudsters.[162] Therefore, data protection is like the 'mark' which represents the protection of personal information but which is limited in utility until we find the 'calabash', a viable identity management system, from which we can verify and authenticate identities. In essence if X says he is Y, it is difficult to disprove it unless the system is dependable in terms of its identity records on X and Y. If it is otherwise, organisations may be protecting 'fictitious, forged or stolen identities.[163]

If this is a correct assessment of the problem, then the underlying question is whether or not there is provision for a unique identification mechanism for individuals in Nigeria. It was noted earlier in this chapter that the Nigeria Identity Management Commission (NIMC) is the central identity management authority in Nigeria. It is relevant here to further highlight some of NIMC's value proposition for the system generally and e-payments in particular. Overall, the NIMC's identity infrastructure, the Nigerian Identity Database

---

[160] IT security expert 1.
[161]The calabash is a product of the gourd plant valued in the African culture for its versatility including use by men for sharing and drinking local wine.
[162] See notes in chapter three which demonstrated that fraudsters have successfully applied for payment cards on other people's account or under false or fictious names. See notes in 3.4.1 Account Takeover Fraud p 70.
[163] IT security expert 1.

(NIDB) serves as a repository of personal information for identification and verification purposes. It is therefore intended to facilitate government and private sector access to common identity needs. For payment systems, the database serves as the basis of implementing the Know Your Customer (KYC) requirement for financial institutions. The national identity card which also operates as bank card combines a person's real world identities with his digital attributes and incorporates three authentication protocols. That is, who a person is (biometrics), what he knows, (PIN) and what he has (the ID card). Therefore, it satisfies the multi-factor authentication requirement for online financial services and may function as a single sign-on for multiple applications. Invariably, it also avoids the proliferation of payment cards, passwords and PINs. [164]

Based on the above discussion, one could argue that since the national identity card discussed earlier in this chapter incorporates individuals' unique identity information particularly their biometrics, it could serve as a unique identification token. Correspondingly, the NIMC's identity database as a central authority for verification of identities operates as a form of Federated Identity Management (FIM) system.[165] This position would be consistent with government objectives to provide unique individual identifier, a national database, and an interoperable and secure identity management system.[166] However, if one accepts that in theory, a central identity system is needed, it will also be relevant to outline the practical challenges of such a system. To illustrate, it is trite that the risks of centralised identity management systems correspond to its advantages, and that the larger the identity databases, the more its susceptibilities to hacking. Therefore, as a central identity management system, the NIMC database is already a viable resource for attack. This problem is aggravated by the fact that government has failed so far to harmonise multiple and parallel identity management programs in the private and public sectors.

---

[164] See generally National Identity Management Commission (NIMC), 'National Identity Management System Project Enabling Cashless Nigeria Policy of the CBN' (2013)<https://www.nimc.gov.ng/sites/default/files/value_proposition_cashless_economy.pdf>accessed 11/04/2015.

[165] In FIM systems, businesses rely on an identification process performed, and identity information provided by a third party, see Information and Privacy Commissioner of Ontario, 'The New Federated Impact Assessment (F-PIA) Building Privacy and Trust-enabled Federation' (2009) <https://www.ipc.on.ca/images/Resources/F-PIA_2.pdf.>accessed 11/04/2015.

[166] See Presidential Implementation Committee on the National Identity Management System (n 164).

As demonstrated by earlier arguments in this chapter, different organisations, both within the private and public sectors, implement identification programs on a need to know or ad hoc basis. It is argued further here that although central identity management implies increased security risks and cost, the risks are compounded by the continued existence of parallel identity management programs. For example, similar to the NIMC's database, databases of personal information operated by banks under the CBN BVN program can be subverted for identity theft and fraud. Furthermore, theft or corruption in one database may render information in other databases unreliable. It is also quite possible to register with different identity information on different databases. While biometrics may aid identification in such cases, it is possible for biometrics to be replaced or otherwise compromised on one database to render it unreliable for identification in others.[167] To underline the security complexities and cost implications of large identity databases, it was aptly noted as follows:

> Any system that supports critical security functions must be robust and resilient to malicious attacks, because of its size and complexity, the identity system would require security measures at a scale that will result in substantially higher implementation and operational costs... the proposed use of the system for a variety of purposes, and access to it from a large number of private and public sector organisations will require unprecedented attention to security.[168]

Conclusion

The analysis in this chapter outline the relevance of laws to the protection of personal information which may be used for identity related cybercrimes. The arguments also outline the threats posed by multi-stakeholders engagement in e-payments and the danger of divergent notions of personal information. It was argued that although the Nigerian constitution protects privacy, the constitutional provisions are inadequate to protect personal information because the concept of personal information is both broader and narrower than the concept of privacy. An examination of the definition of personal information in respective sectors particularly banking and telecom also suggests that the data protection guidelines developed by industry is inadequate. The concept of personal

---

[167] See further notes in 6.4.1.3 Security is never "Absolute" p 192.
[168] Davies, Hosein & Whitely, 'The Identity Project; An Assessment of the UK Identity Cards Bill and its Implications' (2005) The LSE Identity Project Report 2005 5, <http://eprints.lse.ac.uk/684/1/identityreport.pdf>accessed 11/04/2015.

data lacks uniform definition which precipitates the conclusion that what constitutes personal data differs according to industry and organisation. Using the definition proposed by the draft law, the analysis further highlight the problematic areas of the concept of personal information, and the need for legal clarity particularly in view of unclear conceptions about privacy and data protection in Nigeria.

The chapter concludes with the identification of the administrative and enforcement challenges of a data protection law in Nigeria. It was argued that based on the analysis of the empirical data, lobby interests, and widespread non-compliance could undermine the passage and effectiveness of the law. Crucially, the analysis identified deficiencies in present identity management systems in Nigeria and how these may facilitate rather than prevent identity-related cybercrimes.

Chapter Six

Theories of Regulation in Cyberspace

Introduction

The analyses in chapters three, four, and five demonstrate that e-payment systems are yet to be regulated by the law in Nigeria. The arguments further demonstrate that although proposals have been made for legal regulation which would control identity-related cybercrimes, these have not transformed into laws. Therefore, the control of identity-related cybercrimes in e-payment systems is left to self-regulatory initiatives developed by the financial industry. It is argued in this chapter that self-regulation is both ineffective and inefficient in controlling identity-related cybercrimes. In order to underpin the primacy of legal regulation, this chapter introduces the theoretical frameworks that explain the significance of laws to regulation of the internet and the activities it mediates.[1]

The chapter begins with a brief examination of the concept of regulation. It then considers the cyberlibertarian and Cyberpaternalists' theories of regulation of cyberspace as well as Lessig's theory of modalities of regulation. It will be argued in the chapter that Lessig's theory is a useful mechanism for understanding not only why legal regulation is imperative but also how the law regulates effectively in cyberspace. Based on the literature and the empirical data, it will also be argued that the theory is relevant for assessing the adequacy of the payment industry's self-regulatory mechanisms to control identity-related cybercrimes in Nigeria. Lessig's theory will therefore be used to explain the limits of technology and industry self-ordering systems in the Nigerian e-payment industry. The chapter will conclude with the exposition of how the theory translates to effective legal regulation in the context of e-payment systems in Nigeria.

6.1 Regulation Generally

The meaning and scope of regulation is varied and contested. According to Morgan and Yeung, 'regulation is a phenomenon that is notoriously difficult to define with clarity and precision, as its meaning and the scope of its inquiry are unsettled and contested.'[2] It would

---

[1] Examining the theories is consistent with the grounded theory approach in this research; see in particular explanations on how theories elucidate the research data. See notes in 1.6 Data Analysis at p 12 particularly at 13 .

[2] Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation* (CUP 2007), 3.

therefore be impossible to cover all definitions and theories of regulation in this thesis. For the purposes of the arguments here, it is more useful to examine the narrow and broad senses in which regulation is understood. In the narrow sense, regulation refers to formalistic legal rules aimed at controlling the behaviour of entities or individuals. For example, Selznick defines regulation as 'a sustained and focused control exercised by a public agency over activities that are valued by a community.'[3] This implies regulation by law or at least by state appointed actors with the objective that the larger society benefits. In a broader sense, regulation is referred to as any form of behavioural control whatever its origin.[4] This notion of regulation includes both state and non-state actors. Therefore, according to Baldwin, Scott and Hood, a broader view of regulation would entail thinking of regulation in three different senses. In the first sense, regulation can be thought of as a specific set of commands which involves the promulgation of binding rules to be applied by a body devoted to the purpose. In the second sense, regulation could be a deliberate state influence which encompasses all state actions designed to influence business or social behaviour. In the third sense, regulation may be understood as all forms of social and economic influence which would include all mechanisms affecting behaviour whether they are state based or from sources such as markets or self-regulatory mechanisms in professions or trade.[5]

The definitions above suggest that regulation could originate from formal laws made by the state or from informal arrangements such as those derived from social norms or devised by markets, or profession or industry. However, while formal and informal rules are both sources of regulation, it has been argued that they have different efficiency levels in the way they affect or modify the behaviour of the regulatory target. Lennes for instance argues that intentionality or deliberateness is essential for adjudging whether an activity is regulatory or not in the first place.[6] In other words, to constitute effective regulation, there must be a deliberate or conscious effort to bring about a regulatory end.[7] Lennes arguments suggest that informal regulatory initiatives are often diffuse and may lack intentionality or deliberateness of those designed by law. This argument would be correct if as Baldwin,

---

[3] P Selznick, 'Focussing Organisational Research on Regulation' cited in Anthony Ogus, *The Legal Form and Economic Theory of Regulation* (Hart Publishing 2004) 1.
[4] ibid.
[5] Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation Theory, Strategy and Practice* (2nd edn OUP 2012) 3.
[6] Ronald Leenes, 'Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology' (2012) 5(2) Legisprudence Tilburg Law School Legal Studies Research Paper Series No. 10/2012 143, 149.
[7] ibid.

Scott and Hood also opine, regulation is the deliberate supervision of private activity in the interest of public rights, interests and welfare.[8] In effect, the objective of regulation must include the general protection of public interest rather than the narrow or sectoral interests of a profession or industry. As to how to design such regulatory frameworks and to ensure their legitimacy, it has been suggested that consideration must be given to their standard setting capacity and behaviour modification attributes. Accordingly, Black defines regulation as:

> … the sustained and focused attempt to alter the behaviour of others to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information gathering and behaviour-modification.[9]

Black's definition underlines the standard setting and behaviour modification nature of regulation. Although she also argues that regulation is not necessarily confined to the state, Black suggests that formal or legal rules are better at achieving standard setting and modifying behaviour. Therefore, as she concludes, even when non-state actors such as social norms or technologies influence how regulatory systems operate, and while regulatory system might harness these towards a regulatory end, they do not in themselves constitute regulation.[10]

In addition to standard setting, the notion that an activity is regulatory also indicates that infringement of standards attracts sanctions or punishment. This, it has been argued, is also often more noticeable in state or formal regulatory regimes. As Ogus points out, if the term 'regulation' is used to denote law which implements collectivist system, then it must be taken that regulation contains the idea by a superior authority, which is the State. It therefore has a directive function and compels individuals and groups to behave in particular ways with threat of sanctions if they do not comply. As a public law therefore, it enforces obligations which cannot be overreached by private agreement, because the state plays a central role in its formulation.[11] Balwin, Cave and Lodge also identify legislative mandate as the one of the five criteria which collectively constitutes the benchmark for assessing good regulation. According to the authors, legislative mandate implies that a regulatory framework derives authorisation from an elected legislature. A further criterion identified by

---

[8] Baldwin, Cave and Lodge, (n 5), 3.
[9] Julia Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 20.
[10] ibid.
[11] Ogus, (n 3), 2.

the authors is accountability and control which underlines the need for regulators to be properly accountable and controlled. The third criterion which must be satisfied by a good regulatory regime is due process which presupposes support for regulation because the procedures are fair, open and accessible. Regulatory expertise which means trusting regulator judgement based on specialised knowledge, skills and experience was identified as the fourth criterion. Efficiency of the regulatory regime is the final criterion for assessing good regulation. Efficiency implies that legislative mandate of a regulatory regime is being implemented effectively.[12]

If the above views of regulation are correct, then one may argue that within the framework of a broad theory of regulation, non-state actors have regulatory roles and their activities may constitute regulation. However, it would also be possible to argue that to be effective, informal regulatory mechanisms initiated by non-state actors must be deliberately and intentionally put in place for public interest purposes. One could further argue that similar to legal regulation or regulation by the state, regulation by non-state actors must contain clearly defined rules which set standards and attach sanctions and punishment to non-compliance. More fundamentally, to be legitimate, good regulation must meet the criteria of legislative mandate, accountability, and due process, expertise and efficiency set out above.

It will be argued later in this chapter that non-state regulatory actors are incapable of meeting these criteria. However, to elucidate the concept of regulation in the context of the internet, the following sections examine theories of regulation in cyberspace and how they aid the understanding of the limits of industry self-regulation in the area of controlling identity-related cybercrimes.

6.2 The Cyberlibertarian and Cyberpaternalist Theories of Regulation in Cyberspace

The nature of the legal problems in cyberspace and how they should be regulated has attracted diverse and contested approaches. Barlow, Post and Johnson articulate the philosophy of the cyberlibertarian school of thought, a pervasive philosophy in the early stages of commercial use of the internet. The fulcrum of the libertarians' argument is that cyberspace ought not to be regulated because regulation is impossible, futile and illegitimate. Barlow argues that because of its transborder nature, cyberspace is inherently autonomous and therefore manifestly unregulable. Also, because it defies attempts by sovereigns and nationalities to govern it, Barlow declares complete independence for cyberspace and

[12] Baldwin, Cave and Martin, (n 5), 25-39.

recommends governance built on democratic negotiations among the (net) citizens. As he asserts;

> You [the government] are not welcome among us. You have no sovereignty where we gather….Your legal concepts of property, expression, identity, movement, and context do not apply to us…we believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge…We must declare our virtual selves immune to your sovereignty…[13]

Post and Johnson make similar arguments. They contend that cyberspace is a different environment where legal and regulatory models applicable to terrestrial activities fail. They argue further that among other factors, this is because the internet disregards physical location, and transactions transcend national borders. According to Post and Johnson, since content, transactions and participants exist, 'everywhere, nowhere in particular and only on the Net,'[14] activities on the internet cannot be mapped to individuals and jurisdictions for regulatory purposes. Regulating cyberspace will therefore lead to conflict of law problems, produce laws having extra-territorial effects and promote regulatory arbitrage and evasion.[15]

As the authors theorise for example;

> Banking and securities regulators seem likely to lose their battle to impose local regulations on a global financial marketplace. And … face serious challenges in seeking to intercept the electrons that transmit the kinds of consumer fraud that, if conducted physically within the local jurisdiction, would be easier to shut down.[16]

Cyberlibertarians conclude that for the internet, a bottom–up or self-regulatory model of control built around principles of freedom and society and expressed as rules established by the market, networks and users should be adopted. Summing up the libertarian position, Myszeweski notes that 'Cyberlibertarians dream of a utopian world in which the internet allows the free market to thrive without any government intervention, communities are bound by common beliefs and values rather than geographical location, and government

---

[13]John Perry Barlow, 'A Declaration of the Independence of Cyberspace' https://projects.eff.org/~barlow/Declaration-Final.html accessed 27/06/2014.
[14] David R Johnson and David Post, 'Law and Borders -The Rise of Law in Cyberspace' (1996) 48 STAN L REV 1367, 1375.
[15] ibid.
[16] ibid 1372-1373.

hold little if any power over the people.'[17] This view of regulation corresponds to the notion that in the broad sense, regulation involves either state or non-state actors. However, the relevant question is whether this approach to regulation also satisfies the criteria for good regulation. For example, to what extent are the rules deliberately and intentional put in place for public interest and welfare?

Cyberlibertarian are criticised particularly by alternative explanations offered by the cyberpaternalists. Stated simply, the crux of cyberpaternalist argument is that the internet as a medium of communication or commerce places no limits on the regulatory powers of national governments. They contend that states have a legitimate duty to protect their citizens from harm on the internet as everywhere else.[18] As Wu argues, the notion of a free internet promoted by cyberlibertarians is deeply flawed in the first place. He contends that much of what is considered the free internet was privately regulated from the beginning through technology such as firewalls deployed by corporations. The idea of a free internet is therefore largely inaccurate and illusory.[19] Shapiro concurs with this view when he observed that the internet was neither inherently democratic, nor an automatic guarantor of liberty or fairness.[20]

The cyberpaternalist arguments suggest that for the internet, rules were not deliberately or intentionally made but are inherent to the technology or architecture of cyberspace. If this position is correct, a further and logical suggestion would be a need to moderate the self-evolving rules to serve a regulatory end such as the protection of users of the internet. As demonstrated above, the cyberlibertarian position excludes such moderation by the law or the state but rather implicates the users and markets as agents of self-regulation. However, one must ask that if the market and users ordinarily assume regulatory roles, to what extent can they be expected to develop rules that protect their shared rather than respective interests? Weinstock and Gillen make useful arguments regarding this question.

According to Weinstock, the libertarian concept of self-regulation is both infeasible and undemocratic because a bottom-up approach cannot develop given the insurmountable collective action problems online. In other words, because formulating a global norm is

---

[17] David Myszeweski, 'Cyberlibertarianism in the Silicon Valley' (2003) vol xxxi(5) The Stanford Review.
[18] See eg Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65(4) The University of Chicago Law Review 1199.
[19] Timothy Wu, 'Cyberspace Sovereignty? – The Internet and the International System' (1997) 10(3) Harvard Journal of Law and Technology 647, 653.
[20] Andrew L Shapiro, *The Control Revolution How the Internet is Putting Individuals in Charge and Changing the World We Know* (Century Foundation 1999) 14.

difficult if not impossible, participants online cannot support their visions of self-governance.[21] Therefore, a free sovereignty in cyberspace cannot emerge at all without the backing of the territorial liberal state.[22] More fundamentally, Weinstock contends that because of the propensity of market to dominate in self-regulatory schemes, libertarian notions of regulation will fail to effectively guarantee the rights of users. Conversely, liberal states, with experiences of guaranteeing such rights offline, would be more effective at doing the same online. He concludes that state regulation of cyberspace is necessary for the protection of democratic ideas. As he argues, '[an] untrammelled cyberspace would prove inimical to the ideals of democracy and …state regulation of cyberspace is warranted to promote those ideals.'[23]

Weinstock's correct assessment is that because of the democratic values at stake, the state is an essential participant in formulating regulation for the internet. This argument becomes more persuasive if one considers the limitations on users when it comes to their abilities to either identify or formulate coherent rules to protect those rights. As Gillen also correctly argues, the rights at stake need to be identified in the first place and expecting user-groups to resolve the dilemma in the way cyberlibertarians suggest is unrealistic.[24] In this respect, she notes as follows:

> Self-regulation mechanisms can work quite well, but only where there is a clear context and description of the rights and obligations involved….[since] it is not clear, how user-led cyber-democracies of their own, can create a functional and legitimate rights enforcement mechanism,…An assertion that this will evolve organically will not actually cause this to happen and it certainly will not cause it to happen in a sustainable and appropriate way.[25]

If the above is a correct assessment of users' ability, then it would also be correct to assert that technology and the market are the only determinant of what rights are at stake and how to protect them. Conversely, since market systems or self-regulation allows individuals and groups to pursue their own welfare goals, it promotes the primacy of sector, individual or group interests. Therefore, without legal determination of users'

---

[21] Neil Weinstock Netanel, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88(2) California Law Review 395, 405.
[22] ibid 488.
[23] ibid 403.
[24] Martina Gillen, 'Lawyers and Cyberspace: Seeing the Elephant?' (2012) 9(2) Scripted 131, 135.
[25] ibid 136.

rights and legal regulation of the market, the market can become dominant and manipulative, and may even fail. (Legal) Regulation is therefore justified on the grounds that it is required to produce behaviour which is consistent with the protection of users' rights.

Finally, with specific reference to criminal activities, it is possible to argue that the utility of libertarian arguments is relative to time and context. For example, much of the cyberlibertarian philosophy was influenced by concerns for freedom of speech and censorship which may result from content regulation. As Perrit argues, conventional (libertarian) thinking about internet regulation was driven by the suggestions that freedom of speech and the press protected by liberal democracies could only be enhanced by freedom of the internet. Consequently, the idea of internet regulation was associated with autocratic regimes.[26] However, since commerce and its implications for privacy and fraud was a late comer to the internet, it is also arguable that much of earlier libertarian arguments fail to effectively evaluate the risks posed to e-commerce. This development (of e-commerce) shows that there is as much, if not more, concern about crime online as there is concern about liberty and freedom. Cyberlibertarians therefore miss an important point, that is, without government oversight, cyberspace will become the haven of criminals because neither market nor individuals have control over criminal activities in terms of jurisdiction, arrests or prosecution or punishment. In this context, self-regulation would be no regulation at all.

The foregoing arguments underline not only the possibility but also the imperatives of legal regulation of the transactions and activities on the internet. However, on account of the complex technical environment of the internet, simply conceding to legal regulation does not explain how that regulation is to be structured or implemented. For example, with few exceptions,[27] cyberpaternists often express commitment to legal or state regulation without outlining a modality or approach workable in the context of the internet. Consequently, paternalists have argued that because cyberspace is not an isolated sphere for law and regulation, it must only be understood in the context of wider principles of law and regulation. Easterbrook contends for instance, that having a separate law on cyberspace is

---

[26] Henry H Perrit (Jr), 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strenghtening National and Global Governance' (1998) 5 Indiana Journal of Global Legal Studies 423.

[27] See eg Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76(3) Texas Law Review 553; see also Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

no different to having a 'law of the horse'.[28] This position concedes to law but rather old laws than new ones. Also, by their own admission, writers like Goldsmith simply set out to demonstrate that regulation of cyberspace is feasible and legitimate, but not to argue that such regulation is efficient or democratic.[29] Therefore, having argued that law is essential to regulation in cyberspace, it is also important to commit to an approach of how legal regulation is to be implemented effectively. Lessig's theory of modalities of control provides further explanations not only for why law is an effective regulator but also on how it regulates on the internet. The following sections summarises the main points of Lessig's proposal.

6.3 Lessig's Theory of Modalities of Regulation

Lessig identifies four modalities of regulation or 'things that regulate' in real space. [30] These are law, architecture, norms and market. He argues that these modalities as constraints to behaviour in real space are transposable to cyberspace. According to Lessig, law constraints objectively because it provides a set of commands and threatens punishment for disobedience. As in real space therefore, the constraints of law in cyberspace is the threat of sanctions for violations of certain rights or punishment for certain behaviours.[31] Norms or social norms also constrain, although differently from law. Lessig posits that normative constraints are imposed through slight and sometimes forceful sanctions imposed by members of a community on each other rather than by organised or centralised action of the state. [32] Correspondingly, norms regulate the internet because behaviour can earn the disapproval of other users as contravening the norm of certain online fora.[33]

It is important to note from the outset that while instructive, Lessig's conception of norm regulation is problematic. In the sense that Lessig defines them, norms are socially constructed set of constraining rules accepted by a community of users. Norms, Lessig argues, stops people from smoking in a private car without first asking the permission of other passengers because there are no smoking police or smoking courts.[34] In the context of electronic transactions however, it is difficult to understand what norms can develop or how

---

[28] Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) U. CHI. LEGAL F. 207, 207-216.
[29] Goldsmith, (n 18) 1201.
[30] Lawrence Lessig, *Code Version 2.0* (Basic Books 2006) 120.
[31] ibid 123- 125.
[32] ibid 340-341.
[33] ibid 123-125.
[34] ibid 122.

they will operate. For example, the proposal of regulation by norms would beg the question of how generally acceptable norms would develop in the first place. As argued above, it is difficult if not impossible for users to identify and articulate rights which require protection online.[35] This is particularly so since the cultural specificity of norms and the relativeness of individual choice, as well the fluidity and mobility on the internet negates the permanence of engagements needed to sustain the development of generally acceptable norms. According to Goldsmith, the idea of a global norm would often be unattractive as several billion of people using the internet would not agree on regulatory norms. [36] Notably, even Lessig could not provide specific examples of normative responses. He noted rather vaguely that 'Norms could be used to respond to these threats … Norms among commercial entities, for example, could help build trust around certain privacy protective practices.'[37] However he fails to provide any clues as to how the norms will develop. Rather, he concedes that, 'how people who need never meet can establish and enforce a rich set of social norms is a question that will push the theories of social norm development far.'[38]

The observations above suggest the need for accuracy and clarity in problematising the respective modalities of regulation. As an alternative to the contested notion of collective norms therefore, the analysis here opts for the term 'users'. 'Users' is a more specific term which underlines the fact that the problem surrounds a group of people more likely to make individual rather than collective decisions. In the particular context of e-payment systems, it addresses the ability or inability of respective users to articulate their choices in view of the payment instruments, processes and providers they choose. Furthermore, on account of their susceptibilities to social engineering, users are invariably part of the problem, it is proposed here to make them part of the solution. In other words, the term elucidates the role of users as part of the solution within Lessig's regulatory proposal. Murray's observations to the effect that users are not to be considered as passive recipients of regulatory initiatives support this point.[39]

As mentioned earlier, Lessig identified the market and architecture as further modalities of regulation. As Lessig argues, the market, as the third modality of regulation, constrains

---

[35] See arguments made following Weinstock and Gillen above.
[36] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a borderless World* (OUP 2006) 152.
[37] Lawrence Lessig, *Code Version 2.0* (n 30) 223.
[38] Lawrence Lessig, 'The Zones of Cyberspace' (1996) 48(5) Stanford Law Review1403, 1407.
[39] Andrew D Murray, *The Regulation of Cyberspace Control in the Online Environment* (Routledge Cavendish 2007) 51.

through differential pricing. This is based on the fact that prices signal the point at which a resource can be transferred from one person to another.[40] The fourth modality of regulation is the architecture of an environment which encompasses either the way things are or the way they are made or built.[41] In the context of regulation, architecture can enable or limit interaction with the environment, but unlike the other three constraining modalities, architecture is independent of direct human imposition, and is often automatically deployed or self-executing.[42] Correspondingly, the architecture of cyberspace is its code.[43] Code is the software and hardware that makes cyberspace what it is and includes built-in architecture such as its foundational and operating protocols, as well as designed controls such as encryption technology, tracking software, and access and authentication protocols such as PINs, passwords and access codes.[44] Like real space code, the code of cyberspace is self-executing. Similar to a locked door which shuts one out irrespective of one's wishes, the code of cyberspace such as encryption, passwords, and access codes deny the outsider access to confidential information. Therefore, in contrast to laws which do not punish people for unknown offences, and norms which are widely known and accepted within communities, code constrains without objectivity and operates whether or not the party being constrained is aware of it.[45]

As Lessig further argues, because of the self-executing and independent nature of code regulation, the application of law or legal constraints in cyberspace is inherently limited. He notes that 'Various "trusted systems" – permit a far more "fine –grained control over access to and use of protected material than law permits, and can do so without the aid of the law."[46] To that extent therefore, code has regulatory potentials similar to and analogous to regulation by law and indirectly or metaphorically, 'code is law'.[47] However, Lessig argues, most persuasively, that because code can control better and more effectively than law, it may be misused particularly by the market. As a result, code may not strike the balance or protect the various values prescribed by law and may become quite arbitrary in application. For example, code may be used to block otherwise lawfully available access or content such as in cases where the holder of copyright uses technology of trusted systems to inhibit fair

[40] Lessig, *Code Version 2.0* (n 30) 123-125, 341.
[41] ibid 342.
[42] ibid.
[43] ibid 341-343.
[44] ibid 124-125.
[45] ibid 341.
[46] ibid 127.
[47] ibid 5.

use or to protect his right beyond the limits prescribed by law.[48] Code could also be used to collect personal information without the knowledge and/or consent of the user that the information is being collected. [49] The malicious and criminal use of encryption is a further example of misuse of code. As was argued in chapter three, encryption could be used to mask legitimate as well as criminal communication including the anonymity and intractability of fraudulent transactions.[50] Lessig's argument is therefore that code is not always a positive regulator and does not always constrain in a manner which promotes the law, and may infact override legal control. Wu makes the point more forcibly by asserting that code could be used as a mechanism of avoidance rather than of change.[51]

The foregoing arguments are correct and underline the fundamental problem with regulation by code or technology in e-payment systems. As further arguments below demonstrate, code application may cover all forms of industry malpractices including failure to apply correct security and authentication protocols. It may also constitute the basis upon which organisations deny liability for fraud arising from their own omissions. Conversely, code can effectively constrain users by preventing them from engaging in practices that undermine their own security. It is therefore accurate to say that without further moderation of the code's pervasive regulatory capacity, its effect is to completely override individual, corporate or government decision making.

Accordingly, Lessig proposes direct regulation either of the code of cyberspace itself, or of the institutions that produce the code.[52] As an overriding regulatory modality, Lessig argues that law can modify, alter or enforce the code of cyberspace in a way which promotes the demands of commerce, society, policy and justice. [53] The same argument applies to regulation of other modalities of market, and norms. Lessig concludes that law is the 'most obvious self-conscious agent of regulation',[54] and will affect the other modalities in a way which aids their roles as tools for legal regulation.[55] As Lessig concludes, the key policy in cyberspace is a proper mix of the modalities of regulation. Notably, the mix need not

---

[48] See eg Mark Stefik, 'Shifting the Possible: How Trusted Systems and Digital Property rights Challenge Us to Rethink Digital Publishing' (1997) 12 Berkeley Tech LJ 137.
[49] Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) Harvard Law Review 501, 519-520.
[50] See notes in (d) Public Key Infrastructure (PKI) p 82.
[51] Tim Wu, 'When Code isn't Law' (2003) 89 Virginia Law Review 101, 106.
[52] Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (n 49) 514.
[53] ibid.
[54] ibid 511.
[55] ibid 502.

operate in a set form or order. The order may differ depending on the behaviour or activity which is the focus of regulation.[56]

It is important to mention that although Lessig's approach to regulation in cyberspace has been approved as correct,[57] it has also been variously criticised.[58] In fact Murray offers an alternative theory to resolve the regulatory problems online.[59] Murray's concept of 'polycentric regulation'[60] implies that a network of regulatory actors operate in cyberspace. Murray argues that regulation rarely, if ever emanates from a single regulatory source. He also concedes that the malleability and flexibility of the environmental architecture (or code) increases the susceptibility of the space to regulation. However, in contrast to Lessig, Murray argues that because of the complexity of cyberspace and the attendant regulatory web it creates, regulation would fail to produce predictable outcomes in cyberspace. As he contends, while unpredictability can be reduced because of the inertial of the environmental modalities of real or physical space, the malleability of the layered and complex environment of cyberspace makes it difficult to predict the effects of regulation.[61] In effect, Murray expresses doubts that the regulatory modifications to the environmental modality (the cyberspace code) will produce the expected regulatory effects anticipated by Lessig. He argues that this is because any change in the 'regulatory web' can have immeasurable consequences and make it impossible to determine the effects of even minor changes on the regulatory subject. As to whether this implies that all regulatory attempts are doomed to failure, Murray's simple answer is a no.[62] His alternative is a dynamic matrix theory, which is a model of network communitarianism designed to assist regulators in mapping when external regulatory interventions could be effective.

According to Murray, the active matrix model requires the replacement of Lessig's isolated pathetic dot with a networked community or matrix of dots which has shared ideals, beliefs and opinions. The model also entails the need to recognise that social modalities of law, norms and market draw their legitimacy from the community of dots. Therefore, the model

---

[56] Lessig, *Code Version 2.0* (n 30) 224.
[57] Eg Reidenberg first proposed 'lex informatica' or law of information which is analogous to Lessig's theory of code regulation. See Reidenberg, (n 27) 556-568; see also eg Jonathan Zittrain, *The Future of the Internet: And How to stop it* (2nd edn, Penguin 2009).
[58] See eg Viktor Mayer-Schonberger, 'Demystifying Lessig' (2008) Wisconsin Law Review 713, see also David G Post, 'What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace' (2000) 52(5) Stanford Law Review 1439.
[59] Murray, (n 39).
[60] ibid 47.
[61] ibid.
[62] ibid 227-229, 250.

matrix would suggest that the regulatory process is in nature a dialogue instead of externally imposed set of constraints.[63]

While Murray provides useful insights into the complexity of regulation in cyberspace, and underlines the significant role of users within the active matrix,[64] fundamental flaws of the model include its seeming recourse to the libertarian position and its complexity.[65] For example, the model is built around a complex system of technical assessments and feedbacks and even Murray cautions regulators to be willing to 'take a leap of faith' in the uncertain and unpredictable regulatory environment of cyberspace.[66] From the perspective of a developing digital society like Nigeria, a complex regulatory approach implicates cost and assumes regulators' expertise in the technicalities of cyberspace workings. This by itself may disincentive regulatory initiatives. Concerning his suggestions that legitimacy resides with the community, Murray's later modification and/or simplification of the active matrix model highlights the weakness of the argument. As he concedes;

> It surely cannot be true that the general will of the people, lacking the imprimatur of legitimacy that is to be found in legislative assembly, can simply decide which laws are "valid" and which are not. The danger of the active matrix theory is that it comes perilously close to suggesting mob rule for cyberspace… Equally it never was my intent to suggest, in the style of cyberlibertarianism, that the will of the community overcomes the will of the legitimate external regulator. Rather it was about modelling responses to regulatory interventions in an attempt to model the high rate of regulatory failure in cyberspace.[67]

In Murray's view and consistent with the proposal in this thesis,[68] it is undesirable and counter-productive to undermine the role of the law, rather what should be done is to suggest models for how law could work more effectively.[69]

---

[63] ibid 234- 251; see also Andrew D Murray, 'Nodes and Gravity in Virtual Space' (2011) 5(2) Legisprudence 195, 206-209, 212 .
[64] See previous notes on the limits of Lessig's norms at p 182.
[65] Murray, *The Regulation of Cyberspace Control in the Online Environment* (n 39) 250.
[66] ibid 250-252.
[67] Murray, 'Nodes and Gravity in Virtual Space' (n 63) 209.
[68] See proposal for cybersecurity in chapter eight.
[69] See eg Chris Reed, *Making Laws for Cyberspace* (OUP 2012); see also Emily B Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24(3) International Review of Law, Computers & Technology 263.

Lessig's theory is therefore preferred because of its simplicity and utility in explaining the challenges of regulating behaviour in cyberspace and the mechanisms for overcoming the challenges. The theory is useful because it provides clarity and pragmatism in that it involves a transposition of real world control mechanisms of law, norms, market and architecture to the internet. It reinforces the notion that although there are new challenges in internet mediated transactions, they are neither unresolvable nor insurmountable. As Agnew and Pyke noted, a good theory must among other things, be simple, testable and predictive.[70]

More significantly, the theory is consistent with the notion that cybersecurity must account for processes, devices, institutions, technologies, as well as users and laws and policies.[71] For the purposes of further analysis here, Lessig's theory provides the basis for validating the assumption that respective regulatory modalities do not work effectively if they are independent of legal regulation. With specific reference to the research data and to policies and practices in the Nigerian e-payment industry, the following sections highlight the respective limits of existing regulatory mechanisms in the e-payment industry. They also demonstrate how lack of legal regulation implies further adverse consequences for developing e-commerce, promoting trust and controlling identity-related cybercrimes.

6.4 The Limits of Technology, Industry and Users in Controlling Identity-related cybercrimes in e-payment systems in Nigeria

6.4.1 The Limits of Technology (Code) Regulation

Chapter three discussed how code or technology is being used to address the problem of fraud. Industry standards, particularly the PCIDSS, and technological solutions including encryption and authentication technologies were examined. As the previous analysis show, these technologies are the most pervasive response to identity related cybercrimes in e-payment systems. This position is consistent with the view that code plays the most important role in the regulation of cyberspace because it is self-executing when it comes to constraining human behaviour. Technological based security systems are therefore of immense importance to users of e-payment services because technology regulates behaviour without requiring users themselves to change their behaviour.[72] However, there are constraints on technology as a modality of control and three clear areas can be identified which may inhibit efficient regulation by technology in Nigeria. These are cost, the industry

[70] Agnew N and Pyke SW, 'The Science Game' cited in Vincent A Amfara (Jr) and Norma T Mertz, *Theoretical Frameworks in Qualitative Research* (Sage Publications 2006) xvii.
[71] See eg definition of cybersecurity at p 85.
[72] See further notes below in 6.4.3 The Law and Regulation of Users.

centred character of technology regulation and the fact that no security is completely impervious to threats.

6.4.1.1 Technology is Expensive

The cost of implementing certain technologies may affect the willingness and voluntariness of industry to deploy them. This is particularly relevant if one accepts the assumption that organisations are profit-centric and may cut security costs to maximise profits. The PCIDSS discussed in chapter three serves as a useful illustration here. It was noted in that chapter that the level of compliance with the PCIDSS in Nigeria is contested.[73] Research offers some indications of why compliance might be a problem. According to one estimate, the cost of fully implementing the PCIDSS for a merchant in Nigeria is about $20,000 USD which is considerably more than the total operating capital of an average merchant.[74] Thereafter, the business needs an additional $1000 per year for payment of software update on electronic points of sale.[75] Merchants also have to bear additional cost of periodic system vulnerability and compliance scan to third party firms appointed by PCIDSS operators to ensure full and ongoing compliance. It was argued that this prohibitive cost can only be borne by the big players in the industry such as banks and switching companies.[76] Invariably, cost represents not only a barrier to entry into e-payment services, but may also lead to compromise of security standards. As noted in the PCIDSS guidelines, prohibitive costs of compliance invariably lead to compromise of consumer information. Therefore, businesses unable to encrypt on account of technical constraints or business limitations adopt compensating controls designed to mitigate associated risks.[77]

It is also notable that problems of compliance are aggravated by lack of regulatory oversight of the PCIDSS. For example, although the PCIDSS requirements are couched in mandatory terms, compliance is determined mainly through self-assessment. Also, while the Security Standards Council (SSC) sets the PCIDSS, there is a lack of uniformity in the implementation of the standards because each card brand has different programs for

---

[73] See notes in 3.5.1.1 Industry Private Ordering System - Payment Card Industry Data Security Standards (PCIDSS) p 74 at 76.
[74] Fidelis C. Obodoeze et al, 'Enhanced Modified Security Framework for Nigeria Cashless e-payment System' (2012) 3(11) International Journal of Computer and Science Applications 189.
[75] ibid.
[76] ibid 189-190.
[77] See Security Standards Council <https://www.pcisecuritystandards.org/> accessed 11/09/2013.

compliance, validation and enforcement.[78] The Council does not therefore have the mandate to validate or enforce any organisation's compliance with the standards or to impose penalties for non-compliance. Enforcement and penalties are governed by card brands and their partners who may impose financial penalties or withdraw card acceptance services.[79] This lax enforcement framework is compounded by lack of independent legal authority to enforce the standards either on behalf of the Council or the card brands.[80] Compliance is therefore implemented through private contractual arrangements between card brands and members of the payment network to which the PCI-Security SSC is not a party.

Therefore, in addition to cost, the fact that the PCIDSS is not a legal requirement affects the level of compliance. If this position is correct, one may argue that legislation is required to codify the requirements of the PCIDSS. A contrary approach would lead to the correct conclusion that the PCIDSS is merely a tool to pre-empt government interference and stem off legal regulation.[81] As Smedingoff rightly observed, three legal trends are currently shaping the landscape of information security. One is that laws are requiring a legal duty to provide appropriate information security for a company's data and electronic transactions. Two, laws are setting legal standards for compliance, and three, laws have evolved a new legal duty to warn the stakeholders affected by security breaches.[82] Indeed, with specific reference to developing countries, Rosenberg cautioned that the effect of failure to legislate to regulate payment card transactions translates to governments effectively ceding consumer protection to private law making by card associations and banks.[83]

6.4.1.2 Technology as Industry Regulation – Misuse in Evidential Matters

Another important aspect of regulation by technology is its near-total dependence on industry for its implementation. As already noted above, code as a tool of market regulation presents its peculiar problems. Infact, in market regulation terms, technology is not necessarily regulation-enhancing and can in fact be used to foil regulation. An example is

---

[78] Edward A Morse and Vasant Raval, 'PCI DSS: Payment Card Industry Data Security Standards in Context' (2008) 24 Computer Law and Security Report 540, 553.
[79] See Security Standards Council <https://www.pcisecuritystandards.org/> accessed 11/09/2013.
[80] Morse and Raval, (n 78), 551.
[81] ibid.
[82] Thomas Smedinghoff, 'It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law' (2007) 16(1) Michigan State journal of International Law 5.
[83] Arnold S. Rosenberg, 'Better Than Cash? Global Proliferation of Debit and Prepaid Cards and Consumer Protection Policy' (2005) Berkeley University Press (Bepress) Legal Series Paper 766.

the (mis) use of technology to collect excessive personal information. It is argued further here that on account of its highly technical nature, the deployment of technology is better understood by industry and this may lead to discriminatory and even abusive use. Although there is no authority on this point in Nigeria, decided cases in England demonstrate that abusive uses of technology by the financial and payment industry can undermine the judicial process and produce injustice.

In Job v Halifax PLC,[84] the claim was for the sum of £2,100 (with interest) which the claimant argued had been wrongfully debited from his account with Halifax bank through the fraudulent use of his debit card. The bank admitted the debt, but argued that they were justified because the money was withdrawn from the claimant's account using his Card and correct PIN. However, in giving evidence, the bank declined to disclose card authentication keys because they were derived from a batch and would compromise other cards in issue. It was argued for the bank that key management procedures were commercially sensitive information and an outside expert witness could not verify the authentication codes in the logs. However, it was contented for the claimant that these pieces of evidence were essential to the bank's claim that the transactions occurred. They were also relevant to prove that the protocols were flawless and tamper-proof and particularly that the bank maintained appropriate security controls on key management. Notwithstanding the failure of the bank to produce the evidence, the claimant failed and judgement was given in favour of the bank. [85]

Similarly in Rahman v Barclays Bank,[86] the claimant sought reimbursement from his bank for money debited to his account in consequence of the fraudulent use of his debit card by a third party. Without putting the defendant/bank to strict proof, the court accepted its explanation that the fraud was committed because the claimant was negligent in that he gave the thief his card and other authenticating information. Also without proof, the court accepted the defendant's assertions about the security of its authentication process and of its electronic banking system. As the court itself observed, 'The bank did not put before the court any detailed evidence about the security information it sought from the fraudster. It had no record of the transaction, save in general terms.'[87] An important factor in this case is

---

[84] (Case number 7BQ00307 30 April 2009) in Alistair Kelman, 'Case Judgement: England and Wales' (2009) 6 Digital Evidence and Electronic Signature Law Review 235.
[85] ibid 238.
[86] Rahman v Barclays Bank PLC (Clerkenwell & Shoreditch County Court Case No 1YE003643 24 October 2012) in Stephen Mason and Nicholas Bohm, 'Commentary on Case on Appeal: England and Wales' (2013) 10 Digital Evidence and Electronic Signature Law Review, 175.
[87] ibid 185.

the fact that the claimant might have prejudiced his case by his alleged untruthfulness regarding the circumstances surrounding the fraud. Nevertheless, as Mason and Bohm argue, the fact that banks could succeed in defending claims by their customers without producing crucial evidence is a disincentive to retain such evidence and produce it when required. Conversely, if the law makes production of such evidence mandatory, banks would have no choice but to retain the evidence. The authors concluded that, 'If their [banks] defence fails for lack of the relevant evidence, they will soon enough learn to make sure to retain and produce it. Soft cases make bad law.'[88]

The above mentioned cases demonstrate how banking and payment systems can be used to manipulate even legal and judicial processes using technology as a shield. Such manipulations could lead to doubts as to whether justice was served in particular cases involving disputed transactions between banks and their customers. While as noted above, cases of this nature have not been decided in Nigeria, the provisions of the Evidence Act give some indications that Nigerian courts may arrive at similar conclusions. For example, although, the Nigeria's Evidence Act permits the admissibility of electronic evidence, there are no laws or rules stipulating the nature and characteristics of such evidence or the burden and standards of proof required in electronic transaction cases.[89]

6.4.1.3 Security is never "Absolute"

As previous arguments in this thesis suggest, service providers often contest the ability of criminals to access their organisations' computer or information systems.[90] Correspondingly, providers deny liability for financial losses to consumers on grounds that the security of the payment processes or instruments are impermeable or impenetrable. Invariably, the arguments tend to be that it is the user or customer who has been negligent in some ways.[91] One service provider underlined the context of this confidence when he contended the alleged compromise of a customer's payment card. As he argues, a customer had alleged that his (the customer's) debit card was used to make fraudulent withdrawals although he (the customer) still had physical possession of the card. Accordingly, the provider concluded;

---

[88] ibid 187.
[89] See ss 93- 97 Evidence Act (Nigeria) 2011.
[90] See notes in 3.3.2.1 Hacking (Unauthorised/Illegal Access to computer Systems) on Hacking p 56 at 57.
[91] See notes in 3.4.1 Account Takeover Fraud p 70.

> The scenario he has just painted is impossible… our cards are EMV cards, they are virtually tamper-resistant, so it's not possible for him to have the card [in his possession] and for someone to access the account at the same time…. They need the card and his PIN. That's why I said we will have problems with people …, many people are dishonest.[92]

One may argue that the above implies that because new payment cards are based on EMV technology, provider organisations may even decline to investigate incidents of card fraud and may simply conclude that consumers have either been negligent or complicit in the fraud. Contrary to the above however, arguments on asymmetric information below imply that providers are in the position to determine how secure their EMV cards are and this information may be known only to the provider.[93] It was also noted in chapter three that authenticators have different degrees of reliability. PINs, passwords, tokens and access codes based on authentication protocols of what a person knows or has, are susceptible to criminal attacks and can be forged or stolen by hackers and phishers. The discussion also outlined the limits of the public key infrastructure (PKI) particularly when they are not supported digital signature laws.[94]

It is important to mention here that while authenticators based on biometrics (or what a person has) are generally rated as providing higher degree of reliability for authentication purposes,[95] biometrics also has security challenges. The technology is particularly relevant because of its increasing and pervasive use for identification in Nigeria. It was mentioned in chapters three and five that the CBN's biometric verification number (BVN) system proposes to authenticate accountholders by matching their biometrics against templates collected by their banks.[96] The NIMC's national identity card and SIM registration by the telecom industry all involve the collection of biometrics as a unique identifier. Therefore, biometrics is poised to play a significant role in identification for political, social and commercial purposes in Nigeria.[97]

---

[92] Payment service provider 4.
[93] See notes below at p 204.
[94] See notes in (d)Public Key Infrastructure (PKI) p 82.
[95] MasterCard, 'Security Matters Insights on Advancing Security and Fraud Management for Payments Spotlight on Biometrics' (MasterCard 2014) 18-22 <http://www.mastercard.com/us/wce/PDF/SecurityMatters_2014.pdf.>accessed 04/06/2014.
[96] See previous notes in (a)Authenticating Technologies p 76; see also notes in 5.1.3 CBN Bank Verification Number (BVN) p 139.
[97] E.g. fingerprint readers were used for voters' identification during the Nigerian general elections in April 2015.

Biometrics is the automated recognition of individuals based on their behavioural and biological characteristics. It is intrinsically bound to a person and can be used to establish identity to a high degree of confidence. Unlike PINs, passwords and tokens, biometrics is permanently mapped to a person and cannot be forgotten.[98] However, biometric characteristics, whether biological[99] or behavioural,[100] also carry the risk of false performance. That is, biometrics can generate false positives and false negatives. False negatives deny access to otherwise authentic users while false positives grant access to fraudulent users or impostors.[101] The failure of fingerprint readers deployed during the Nigerian general elections to identify authentic voters highlights the problems associated with false negatives.[102] In e-payments, e-commerce and e-banking false negatives and false positives carry further implications of financial loss. False negative would lead to payment systems declining otherwise authentic transactions while false positives would grant fraudsters access to victim's financial information or even to organisations' databases.

In addition to the above, biometrics presents problems because of its irreplaceability and permanence. For example, precisely because of its associability with a user, once biometric data is compromised, a person can no longer use the same biometric characteristic to authenticate himself to a particular system and possibly to associated systems. Hence the description of biometrics as a 'PIN you can never change'.[103] More crucially, databases on which biometric information is stored are prone to vulnerabilities and attacks. It was observed in chapter five that the nature of the threat to identity databases includes its very primacy as a target of hackers for identity theft.[104] For example, compromised systems may aid the replacement of legitimate user data with false data or the deletion of stored biometric templates to facilitate re-enrolment.[105]

---

[98] See generally Sanjay G Kanade, Dijana Petrovska-Delacretaz and Bernadette Dorizzi, *Enhancing Information Security and Privacy by Combining Biometrics with Cryptography* (Morgan and Claypool 2012).
[99] For example fingerprints, iris scan, voice or facial recognition.
[100] For example Keystroke and speech pattern.
[101] Alexander D Meadows, 'Spoof and Vulnerability of Biometric Systems' in Eliza Yingi Du, *Biometrics from Fiction to Practice* (Pan Stanford Publishing 2013) 188, 195.
[102] See eg Kim Yi Dionne, 'Why Technical Breakdowns in the Nigerian Elections Raise Questions about Monitoring' *The Washington Post* (Washington, March 29 2015)<http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/03/29/why-technical-breakdowns-in-the-nigerian-election-raise-flags-about-monitoring/ >accessed 12/04/2015.
[103] Russell G Smith, 'Biometric Solution to Identity-related Cybercrime' in Yvonne Jewkes, (ed) *Crime Online* (Willan Publishing 2007) 44, 55.
[104] See notes in 5.4.3 Challenges of Identity Management p 169.
[105] See Meadows, (n 101) 195.

As the above discussion suggests, it is more correct to assume that security compromise is always a possibility. Therefore, as already noted above, industry standards such as the PCIDSS and authenticating protocols such as digital signatures need to be translated into legal requirements. While legal frameworks will not in themselves make security invulnerable, they would provide a basis for accessing compliance and allocating liabilities.

6.4.2 Market Regulation and Constraints of the Payment Industry

Generally, industry initiatives to regulate itself are referred to as private ordering. Private ordering is self-regulation voluntarily undertaken by private parties.[106] It can be made to assuage the specific interests of private groups or to satisfy technical requests. The PCIDSS is an example of private ordering in e-payment systems and services. Although industry standard setting is a rule making process and has a regulatory effect, the analysis here stresses the point that even if industry was willing, it is unable to regulate e-payment to prevent identity thefts and fraud without the coercive force of law. It is argued in particular that market economy considerations create inefficiencies which limit the effects of industry's initiatives and disincline its investment in technological solutions.

6.4.2.1 Market Systems and Asymmetric Information

Information asymmetry exists in markets where information about goods and services are unilaterally known to one party. This may be the seller or the buyer. In any case, markets where information asymmetry exists are characterised by low quality products and high prices because product cannot be distinguished by their characteristics. Where sellers have information for example, the buyers are deprived of the benefit of making informed decisions about prices and quality. In other words, because information about quality is known only to the sellers, prices fail to signify quality to buyers, and sellers of low quality products can sell at prices comparative to high quality ones. This information deficit has two further consequences. First, it drives the sellers of high quality products out of the market because they cannot increase the prices of their products on account of buyers' ignorance about quality. Following the first, the second consequence is the proliferation of bad quality products in the market place leading to buyers' withdrawal from the market and ultimately market failure.[107] Translated into financial and payment services terms, asymmetric

---

[106] See Niva Elkin-Koren, 'What Contract Cannot Do: The Limits of Private Ordering Facilitating a Creative Commons' (2005) 74(2) Fordham Law Review 375, 376.

[107] See generally George Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84(3) The Quarterly Journal of Economics 488; see also Stacey L. Schreft, 'Risks of Identity theft: Can the Market Protect the Payment System? (2007) Federal Reserve Bank of Kansas City Economic Review Fourth Quarterly 5.

information comes into play when providers of payment services promote or disclose the good qualities of their product such as efficiency but withhold the negative features such as insecurity.[108]

Therefore, concerns about information asymmetry are useful for accessing the risk of identity theft. As Schreft argues, since non-cash transactions involve transfer of personal information from the consumer to the seller, the seller's standard of safeguarding information is material to the customers' evaluation of the risk of the transaction. Where there is laxity, the cost of the product should be reduced to reflect the risk of misuse. That is, less secure products should sell for less and more secured product for more. However, because information asymmetry exists, this is not the case. Both secure and insecure products and services sell at relative prices. Providers of less secure products and services will not lower their prices because consumers' associate high price with high quality and sellers of secured products are unable to attract customers desiring such products because of the lack of price differential. Overall, sellers of better security earn a loss while providers of less security earn a profit. Nevertheless, the market as a whole, and not providers of insecure products and services, suffer losses from identity theft. This is because consumers associate losses with the whole market and may migrate to less efficient payment systems as well as because sellers of better security have less incentive to continue to provide such security. This situation precipitates more data breaches, more identity theft and consequently market inefficiency or total collapse.[109]

This discussion can be placed in context by reference to earlier observations about the state of the Nigerian financial market. It was mentioned that issues of fraud are generally shrouded in secrecy.[110] However, this lack of transparency is characteristic of virtually all aspects of banking and financial transactions. These include information about the conditions of the use of financial products, transaction costs and so on. According to the Central Bank of Nigeria;

> An important component of the review exercise was the development of a minimum disclosure requirement that stipulates the information banks are required to disclose to all customers prior to the consummation of every credit transaction. …The overreaching goal … is to produce a Guide that… will

[108] ibid (Schreft) 23.
[109] ibid.
[110] See notes in 3.2 The Challenges of Fraud Reporting p 50.

> accommodate the freedom of operators to charge competitive prices, while protecting consumers from arbitrary and excess charges.[111]

These observations imply that service charges in the financial industry are seldom reflective of value and may be arbitrary regardless of quality. Banking applications and implementation standards for EMV and PCIDSS exemplify how asymmetric information work in e-payment systems. According to Murdoch and Anderson, not only does the security of banking apps vary across platforms and suppliers, but because most apps are proprietary, the vulnerabilities are known only to the service providers. Also, while acknowledging the security of the EMV protocol, the authors argue that the protocol has numerous vulnerabilities which are the inevitable result of implementation choices. Banks can choose for example to issue inexpensive cards that use public key cryptography in the card authentication step or opt for cheaper ones that merely present a certificate signed by the issuing bank. These cheaper cards, which do not use PKI, are easier to clone. [112]

It can therefore be argued, following previous analysis in this chapter and chapter three that since the financial industry in Nigeria barely meets the PCIDSS requirements, and the CBN security requirements under the e-banking guidelines is to be solely implemented and monitored by the banks themselves,[113] consumers may be unaware of banks and other payment service providers with lax security systems. Conversely, products, services and charges could not be comparatively and competitively priced. The CBN itself recognises the effects of asymmetric information on the financial market and has concluded that it leads invariably to distrust and market collapse. According to the CBN, '…customers do not perceive fraud as an issue with a specific bank, but with electronic payments overall, which eventually affects the entire industry and not just the institutions that have been impacted by fraud.'[114]

---

[111] Letter from Central Bank of Nigeria to all deposit Money Banks Reference No CFP/DIR/GDL/01/018 dated 6th July 2012.

[112] Steven J Mudorch and Ross Anderson, 'Security Protocols and Evidence: Where Many Payment Systems Fail' (Financial Cryptography and Data Security Barbados March 3-7 2014 Pre-proceedings Draft) <http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf >accessed 22/06/2014.

[113] For example, banks have different obligations to implement but not to report on their security protocols and they are required to ensure that ISPs implement appropriate security where services are outsourced, see notes in 3.5.1 Central Bank of Nigeria (CBN) Regulations on Privacy and Security p 73.

[114]Central Bank of Nigeria, 'About the Nigeria Electronic Fraud Forum' <http://www.cenbank.org/neff/about.asp> accessed 09/04/2015.

It is however to be noted that as information asymmetry is invariably part of traditional markets, this position is unlikely to change. Organisations expect to protect their brands and withhold adverse information from customers unless they are compelled by law. To correct transactional imbalances therefore, it is the role of government to impose transparency rules. Consistent with this view for example, the UK Payment Services Regulations requires payment services providers to provide their users with information relating to cost, charges, exchange rates, security, and limits on transactions. They must also provide information on liability for fraudulent use of payment instruments, and responsibility to block payment instruments as well as complaint procedure.[115]

6.4.2.2 Market Systems and Negative Externalities

Externalities operate to confer costs or benefits on entities other than those who should bear them. Externalities can be positive or negative. Positive externalities confer benefits on those who cannot be charged for the benefits while negative externalities confer costs on those who should not bear the cost. In markets where the externalities are negative, entities engage more in activities that impose costs on others and less in activities that benefit others.[116] To translate this to the context of e-payments, if risks of insecurities, data breaches and identity thefts and frauds are borne not by payment service provider but by individuals, the society or other organisations, there is less incentive for organisations to provide better security and therefore prevent the operation of negative externalities.[117] Two activities in the Nigerian payment industry show how externalities operate to displace the cost of fraud. Firstly, the liability allocation regime already places the burden of fraud on the consumer or user. Secondly, society through law enforcement appears to have assumed the cost of preventing fraud on e-payment platforms, thus providing further disincentive to industry.

(a) How Unclear Rules about Liability Allocation Promote the Operation of Externalities

It was pointed out earlier in this chapter that organisations engage in liability shifting by arguing that users are to blame for personal data compromise and identity fraud. Invariably, in many cases where conflicts arise as to whether a user had authorised particular transactions, service providers avoid liability either by alleging that users colluded to commit the fraud and subsequently sought to repudiate the transaction, or that they were

---

[115] See generally Part 5 of the Payment Services Regulations 2009 SI 2009/209.
[116] See Richard Cornes and Todd Sandler, *The Theory of Externalities, Public Goods and Club Goods* (CUP 1986).
[117] Schreft, (n 107) 5.

negligent in safeguarding their payment information or instruments.[118] Arguably, even practices put in place by industry to curb fraud inadvertently aid this denial and shifting of liability. A good example is transaction alert system. Under the system, card or account holders receive alerts or notifications immediately a transaction occurs on their accounts or payment cards. The effect is to instantly alert the card or account holder to fraudulent transactions and forestall further fraud. Customers who receive notifications of unauthorised transactions are expected to immediately notify the service provider, which then 'blocks' the account or card to prevent further use by the fraudster.

While seemingly devised to combat fraud and protect customers, the system is also arguably ineffective because it amounts simply to 'bolting the barn after the horse has escaped'. To illustrate, based on already established assumption of negligence or collusion, customers are presumed to be liable for pre-transaction alert losses. The transaction alerts do not therefore significantly affect this existing liability structure. In effect, it does not follow that even if a transaction is fraudulent, the customer would be reimbursed or indemnified for the loss.

The problem described above is particularly aided by lack of specific liability rules applicable to fraudulent and unauthorised payments. As an example, under the E-banking guidelines, determination of liability is subject to the contract between the parties. The Guidelines provide that 'Agreements reached between providers and users of e-banking products and services should clearly state the responsibilities and liabilities of all parties involved in the transactions'.[119] This provision fails to provide any meaningful guidance on the allocation of liabilities and offers little, if any protection to users of electronic banking and payments. It is arguable for instance that while contracts constitute important evidence of the agreement between parties, contracts envisaged by the guidelines will usually be standard form contracts containing extensive exemption of liability clauses. Even if otherwise, users will still generally be incapable of engaging in meaningful negotiation. As discussion on information asymmetry above implies, respective bargaining powers of the parties are likely to be unequal because of service providers' superior knowledge about products functionalities and security defects.

Perhaps in recognition of the inefficiency (and even unfairness) of the present liability allocation structure, the Central Bank of Nigeria proposed a Card arbitration framework called the E-payment Dispute Arbitration Framework. The objectives of the framework include the provision of speedy redress for e-payment dispute complaints without involving

---

[118] See example given above at p 192.
[119] Item 3.0(g) CBN Guidelines on Electronic Banking 2003.

the courts. It is also intended to facilitate the identification of the entity at fault in disputed claims, and to shift the liability towards that entity.[120] Again, however, apart from the fact that the framework is yet to become operative, some of its provisions already suggest that it would be equally problematic and is unlikely to have much effect on the status quo. For example, Item 5(d) of the framework provides as follows:

> *Where a Cardholder uses an EMV Payment Card on an EMV Terminal and fraud occurs, liability is on the Cardholder*. However, it is the responsibility of the issuer to prove to the arbitration panel that the Payment Card issued was the Payment Card used and the Payment Card was not reported stolen.

Upon literal construction, the provisions emphasised above already carry a presumption that the cardholder is liable without requiring that evidence be produced on the state of the security of the service provider's systems. Contrary to arguments above demonstrating that EMV cards can be compromised especially when issuers influence the security designs,[121] the provision appears to suggest that the cards are completely impregnable. As it merely re-asserts the presumption of negligence or collusion on the part of the cardholder, decisions of arbitral panels under the proposed dispute resolution framework will produce results such as Job and Rahman cited earlier.[122] As Mason rightly contends, the resulting decisions would be 'incorrect decisions based on a misunderstanding of the burden of proof, a failure to properly test the evidence, and an acceptance of unwarranted assumptions.'[123]

The Payment Services Regulations (UK) provides an example of how law defines the respective liabilities of parties to a payment transaction. The law places the burden of proving a disputed payment on the service provider and negates presumptions of negligence and fraud on the part of users. [124] Section 60(3) provides as follows:

> Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that—
>
> (a) the payment transaction was authorised by the payer; or

---

[120] See item 3 Central Bank of Nigeria (Proposed) E-payment Dispute Arbitration Framework 2013.
[121] See notes above at p 204.
[122] See notes above at p 191.
[123] Stephen Mason, 'Electronic Banking and How Courts Approach the Evidence' 29(2) (2013) Computer Law and Security Review 144.
[124] Payment Services Regulation 2009 SI 2009/209, regs 60(1)-(3).

(b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 57.

Regulation 57 deals with the obligations of the payer/user to give notification to the service provider of theft or misappropriation or unauthorised use of the payment instrument in the agreed manner without undue delay upon becoming aware of the fact. [125] Therefore the cumulative effect of regulations 57(2) and 60(3) is to displace the presumption of negligence and collusion which often follow a user's allegation of unauthorised use of payment instrument. The payment service provider is put to strict proof even where it appears that the actual payment instrument issued had been used to authorise a disputed transaction.

Furthermore, under section 62 of the Regulations, the law addresses the allocation of liability in instances where the users have been negligent. It provides that the payer (payment service user) is liable up to a maximum of £50 for any losses incurred in respect of unauthorised payment transactions arising from the use of a lost or stolen payment instrument. The liability is the same for losses arising from users' failure to keep the personalised security features of the payment instrument safe from the misappropriation.[126] The user however bears the full liability for the all losses incurred in respect of an unauthorised payment transaction if he has acted fraudulently, or with intent or gross negligence failed to give notification to the service provider upon becoming aware of theft or misappropriation of the payment instrument.[127] The law further provides that the user is not liable for any losses incurred in respect of an unauthorised payment transaction arising after notification has been given to the provider.[128] The user is also not liable where the payment service provider has failed at any time to provide appropriate means for notification in accordance with the provisions of the regulations.[129] The notable omission with respect to the provisions here is failure to define what qualifies as *appropriate means of notification* under Regulations 58(1) (c). However, one may presume that such means of notification will be a medium of communication accessible to the user 24 hours of the day.

The foregoing argument further underline the need for laws to aid the allocation of liabilities when payment is contested and fraud occurs. Significantly, it also demonstrates that laws

---

[125] ibid regs 60(3), 57(2).
[126] ibid reg 62(1)(a)-(b).
[127] ibid reg 62(2) (a)-(b); see also regs 57(1)-(b).
[128] ibid regs 62(3)(a), 57(1)(b).
[129] ibid regs 62(3)(b), (58(1)(c).

could address the fears of service providers that they would be made unjustly to bear the cost consequences of users' negligent or fraudulent behaviour.[130]

(b) Society's Assumption of the Cost of Fraud as Externality

An example of how the society bears the cost of fraud in Nigeria is demonstrated by efforts of law enforcement agents aimed at combatting cybercrimes. Although there are no laws to try the criminals, law enforcement agents appeared to have developed a typology of cybercriminals with the objective perhaps of ultimately preventing the crime through a campaign of scare-mongering. This 'criminal profiling' characterises cybercriminals as male, between the ages of 18 and 33, typically well-educated, (which in the Nigerian context means the person has up to university level education) unemployed and technology savvy.[131] To justify their classification in any of the categories, suspected cybercriminals will also usually be in possession of laptop computers or smart phones with ability to initiate connectivity to the internet almost 24 hours of the day.[132] Such 'suspects' may be classified as 'Yahoo! Yahoo! Boys' (named after the search engine Yahoo), or '419ners' (named after the section of the Nigeria criminal code criminalising impersonation). They may also be classified as engaged in a new form of electronic payment fraud called 'cashless Lagos' in mimicry of the cashless policy of the Central Bank of Nigeria. A successful classification of a person as a cybercriminal is often accompanied by indiscriminate searches of the person, or properties or premises of such persons.

The above practice clearly infringes on certain fundamental human rights. [133] However, the main focus here is how it operates to externalise the cost of fraud. To make this point, it is possible to argue that whereas industry is better positioned to prevent e-payment fraud through deployment of strong technical security, taxpayers appear to pay this cost. For example, while the exercise is arguably wasteful and often futile (because of lack of

---

[130] See eg notes in (a) Personal information is all Information - Why not the Expansionist Approach? p 153 at 154.

[131] This prototype was given by Law Enforcement 1&2; see also UNODC research suggesting that 45 per cent of all global internet users are below the age of 25 and that this majority represents '…a demographic that also broadly corresponds with an age group often at special risk of criminal offending.' See UNODC Comprehensive Study on Cybercrime 2013, 39-42 <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>accessed 02/12/2014.

[132] As the cost of internet connection is still high in Nigeria, the ability to connect to the internet at all hours of the day is deemed a luxury which an unemployed person cannot afford.

[133] For example rights to privacy and freedom from discrimination, harassment and intimidation are guaranteed under s 28(1) (a)-(h) Ch IV CFRN 1999.

cybercrime legislation), government pays for the law enforcement time and resources incurred in the course of indiscriminate searches and arrests. Also, while it is open to industry to contend that law enforcement agents are simply executing their mandate to protect the society, the exercise may also raise speculations that criminals are being arrested and prosecuted. This may in turn prompt suggestions, particularly from service providers, that there is less fraud and therefore less need to invest in fraud prevention.

A correct assessment of the role of regulation in consumer payment systems is therefore that while excessive government intervention in the market could stifle innovation, unfettered markets would fail to produce the right mix of efficiency, safety and access. This is particularly true when payments participants fail to consider all the costs and benefits of their actions to other parties.[134]

6.4.2.3 Inability of Industry to meet the Index for Good Regulation

It is useful to conclude the discussion here by measuring industry attempts to regulate e-payment systems against criteria which may be applied to assess the legitimacy and efficiency of good regulatory regimes. It was noted at the beginning of this chapter that an effective regulatory regime is backed by the cohesive force of law. By necessary inference, regulation which excludes law is inefficient and ineffective. The five criteria outlined by Balwin, Cave and Lodge were also highlighted as collectively constituting benchmarks for assessing good regulation. For ease of reference, these are legislative mandate, accountability, due process, expertise and efficiency.

As the preceding discussions in this chapter and chapters three and five have indicated, the present approach to the regulation of e-payment services cannot satisfy the legislative mandate requirement. This is because the PCIDSS and data protection standards, as regulatory frameworks, are mandated by industry and not statute. Industry also fails to meet the criteria of accountability, and due process or even efficiency in regulation. The general problems of compliance and uniformity of the PCIDSS have been discussed above.[135] In the particular context of Nigeria however, a security expert noted that in spite of the fact that the PCIDSS is a rigorous and on-going process, there are no fully functional monitoring processes in place in Nigeria.[136] Therefore, in spite of the provision of regulatory guidelines that "there will be a continuous review and recertification on compliance with these

---

[134] Barbara S. Pacheco, 'Summary to Conference on Consumer Payment Innovation in the Connected Age' (International Conference on Payment Policy Kansas City March 29-30 2012).
[135] See previous notes at p 189.
[136] IT Security expert 1.

[PCIDSS] and other global industry standards from time to time",[137] organisations are actually accredited on a one-time compliance assessment basis. In other words, after an initial threshold of compliance (for which they receive certificates) there is no framework for periodic examinations to ensure that organisational practices are upgraded. It is trite that the threat landscape for the e-payment industry is volatile, therefore, updating and monitoring compliance is an effective means of ensuring the industry keeps abreast of the risks. Furthermore, as previous discussion in this chapter indicates, although non-compliance with the standards is rife, the process of punishment is not transparent as the industry itself attempts to avoid the stigma or other consequences of non-compliance. As a result, it is difficult to measure the effectiveness of the PCIDSS as a private ordering system.

Finally the establishment of the Nigerian Electronic Fraud Forum (NeFF) serves as a good illustration for the inefficiency of legislative mandate. The NEFF is an all-stakeholder fraud forum established to monitor electronic fraud and encourage fraud reporting, information dissemination and information sharing among stakeholders. As stated in the NEFF annual returns, the forum was borne out of the need for 'a holistic approach to combat the menace of fraud and restore confidence in all e-payments mechanisms in the country.'[138] The rationale for setting up the body include the recognition that electronic fraud attempts will increase significantly as Nigeria migrates to electronic payments, and the fact that e-fraud incidences impact negatively on the financial industry as a whole. The NEFF has as its mandate, the formulation of cohesive and effective fraud risk management practices through information and knowledge sharing with key industry stakeholders. The objective behind the NEFF is to tackle electronic fraud by eliminating the culture of secrecy which makes service providers susceptible to the same types of fraud by the same fraud cartel. The establishment of the Neff is therefore based on the overall assumption that crime control would be more effective if payment institutions share fraud information and articulate a common requirement to law enforcement agents.[139] It is notable that it was the NEFF that provided the statistics indicating that 70% of e-fraud occurrences are attributable to phishing attacks. The NEFF in conjunction with the Central bank of Nigeria and the Nigeria

[137] Item 3.1 CBN POS Guidelines 2011.
[138] Nigeria Electronic Fraud Forum (NeFF) Annual Report 2012.
[139] See generally Central Bank of Nigeria, 'About the Nigeria Electronic Fraud Forum' <http://www.cenbank.org/neff/about.asp> accessed 09/04/2015.

Interbank Settlement Systems (NIBSS) also developed a dedicated portal for fraud reporting in the e-payment industry.[140]

However, while the NEFF is innovative in terms of promoting collaboration, some of its objectives underline the inefficiency and hence failure on the part of financial regulators. Firstly, because the NEFF is projected as an alternative forum of fraud reporting, it is indicative of the failure of primary fraud reporting systems. It therefore impairs the regulators' execution of their regulatory mandate and amounts to re-inventing the wheel. Secondly, and owing to the first reason, its effectiveness is questionable because it is likely to be perceived merely as a regulatory watchdog. One may pose the question for instance that if organisations will not report fraud to the Central Bank of Nigeria (CBN) as a regulator, why would they exchange fraud information at the Neff which is itself an initiative of the CBN and a forum for convergence of competitors, regulators and law enforcement? In other words, it is reasonable to expect that fraud information disclosed at the forum will eventually be passed on to regulators with possible consequences of regulatory reprisals. This would inhibit the free dissemination of fraud information which is the primary objective of the NEFF.

Considered from these perspectives, the NEFF may invariably represent a classic example of the failure of legislative mandate. That is, the NEFF is indicative of the failure of the CBN's legislative mandate to protect the e-payment systems. It therefore appears that industry expertise will be the only strength of e-payment regulation in Nigeria if we apply the index of measuring good regulation. However, it has been argued above that industry can manipulate its expertise to serve its own purposes particularly when using technology. In order to avoid replication therefore, the only point worthy of mention here is that industry may need to be regulated even in how it applies this expertise.[141]

6.4.3 The Law and Regulation of Users

Users' ability to regulate their own behaviour is perhaps the most problematic aspect of controlling frauds and identity related crimes in e-payment systems. From the perspectives of service providers highlighted in chapter five and earlier in this chapter, security is seen more as 'people problem' rather than a legal or technical problem.[142] Generally therefore,

---

[140] See Central Bank of Nigeria, 'Submission of Fraud Report on E-channels using A Common Portal for the Payment Industry' (CBN circular BPS/DIR/CIR/GEN/02/103 of 02 July 2013).

[141] See further notes below on Accountability and the Law.

[142] See example given at p 193; see also notes on (a) Personal information is all Information - Why not the Expansionist Approach? p 153 particularly at 154.

users are considered the weakest link in the security chain. Conceptualising the user problem, it was noted as follows:

> The biggest challenges in information security frequently involve humans…Humans, perhaps unlike technology can demonstrate extreme levels of variation in skill and do not always follow logical rules in conduct. They can be emotional actors, driven by perception and emotion as much as by objective reality.[143]

According to Verizon data breach report, humans are the "the carbon layer" of information assets. They are therefore notoriously susceptible to social tactics including deception, manipulation, and intimidation. The report notes further that while humans are the most complex creatures on earth, savvy threat agents or criminals have consistently outwitted them or otherwise leveraged them to steal data.[144]

A number of reasons account for scepticisms about users' abilities to protect themselves from identity theft and fraud. Firstly, user choices of technical security measures are inhibited by the complex nature of technology and cost. For example, while one may not expect users to implement security at the level of organisations, end-user security measures may be equally problematic in terms of both technicality and cost. In Nigeria particularly, it may be correct to argue that even when available, end-user security measures may be unreliable and defective. As the BSA piracy study shows, PC software piracy in Nigeria at 82% is almost double the global piracy rate which is 42%.[145] It is therefore safe to assume that the Nigerian market is saturated with pirated end-user products including anti-virus programs.

Secondly, and based on the first reason above, users' susceptibilities to crimes increases. This argument holds even when service provider organisations engage in user enlightenment or education. As an example, organisations providing e-payment services particularly banks in Nigeria, have adopted the practice of sending e-mails to their customers periodically informing them of fraud trends and how to avoid victimisation. The following are examples of such e-mails:

---

143 Andrea M. Matwyshyn (ed.), *Harbouring Data: Information Security, Law, and the Corporation*, (Stanford University Press 2009) 229.
144 Verizon, Data Breach Investigation Report 2012, 33.
145 See BSA 2011 Global Piracy Study <http://globalstudy.bsa.org/> accessed 20/09/2013; See also IT News Africa, 'Piracy is Nigeria's greatest Challenge-Microsoft' <http://www.itnewsafrica.com/2012/09/piracy-is-nigerias-biggest-challenge-microsoft/> accessed 20/09/2013.

Dear Valued Customer,

Some of our customers have been receiving Internet Banking Login alerts for logins which they did not initiate. In the alert, they are asked to click on a link for security measures to protect their accounts.

If you receive such a login alert, please be informed that it is fraudulent, and it is an attempt to obtain your banking details.

We reiterate that XXX bank will never require you to click on any link in any communication we send to you. The genuine Login Alert, like all our communication to you, contains no links.

If you do receive a Login Alert asking you to click a link, please disregard and delete it immediately.

Your online security is our priority.

XXX Bank Plc.

Table 6.1- Sample spam login alert

Dear Valued Customer,

We have received enquiries from some customers about transaction alerts purportedly sent by us.

These alerts for strange transactions invite the customer to click on a link to view the details of the transaction. However, the link leads to a 'phishing' site which attempts to get personal banking information such as Internet banking code, password, email address, email password, Phone number, ATM Card PIN, etc.

The following tips will help you identify these fraudulent transaction notifications:

1 The 'Description' contains a link. Do not trust links in an email and DO NOT CLICK on them!

2 The Account Number is masked (e.g. 200 *******) because they do not have that information.

3 The Account Balances are not provided as they are not privy to that information and a wrong figure would prompt you to call your Relationship Officer.

Following these tips will protect you from unintentionally compromising your account.

We reiterate that XXX bank will NEVER request your personal banking details via email and these emails should ALWAYS BE DISREGARDED.

Your online security is our priority.

Thank you for your continued patronage.

XXX Bank Plc.'

Table 6.2 - Sample fraudulent transaction alert

The challenges here include inability to measure the impact of these messages on users and the fact that education cannot keep up with the evolving criminal methods of stealing personal information. For example, increasing use of mobile devices for banking and payments suggests that criminals would migrate to these platforms to leverage attacks. Furthermore, there is disagreement among stakeholders on the utility of this approach to user education. Service providers tend to argue that information about fraud (called fraud alerts) aids education of users on criminal methods used to obtain personal information and represents a means of preventing identity theft and fraud.[146] Other stakeholders take a contrary view and contend that the approach has the capacity to generate negative responses or to "backfire" and has only nuisance value. According to a security expert, it is not only somewhat of a paradox that service providers deny the pervasiveness of fraud, it is also paradoxical that their numerous fraud warnings constitute a form of "user spamming". As he noted;

> …you need to understand ... I'm not saying it is bad to warn your [the banks' customers], but anyone [accountholders in Nigeria] knows these warnings have become so everyday that they are nonsensical or scary. I mean, banks are virtually spamming us [the customers], … and the 'spammers' are spamming us too… As a reasonable person, wouldn't you just stop using the systems [e-payments, e-banking etc.] altogether?[147]

Even if this assessment of user education is incorrect, the invariable inference here is that organisations' attempts to educate users may rebound and result in consumers' either withdrawing from or refraining from using e-payment systems at all.

As previous observations above also underline the fact that users are likely to always be susceptible to manipulations by malicious actors, one can argue that end users cannot be independent regulators because they are volatile and unpredictable actors. Furthermore, because technology generally undermines the capacity for consent online, even attempts to give users substantive control over their personal information through the notion of consent or meaningful choice are replete with pitfalls. Austin argues for example that consent online is really a trade-off between privacy and utility.[148] In Shapiro's view, leaving privacy protection to individuals is inefficient, time-wasting and has the disadvantage of raising

---

[146] all payment service providers interviewed made this point.
[147] IT security expert 2.
[148] Lisa M. Austin, 'Is consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA' (2006) 56(2) University of Toronto Law Journal 181.

transaction costs.[149] Nevertheless, given that users can be ignorant, or negligent, it would still be quite arbitrary for the law to impose limitations on how consumers' transfer their personal information. The CBN Biometric Verification Number (BVN) better illustrates industry recognition of this problem. The BVN system discussed in chapter five appears to have followed the part of technologies that pre-determine users' behaviour by locking them into certain choices.

Lock-in technologies modify or alter the behaviour of actors in ways which ensure compliance with law or regulation. Built-in security processes embedded in privacy by design (PbD) and privacy enhancing technologies (PETs) serve as good examples. PbD embed privacy features into the design specifications, implementation, and networked infrastructures right from the outset. It entails building-in privacy requirements from the onset of a systems' development and throughout its life cycle.[150] Consistent with this approach, and the notion that technology is self-executing when it comes to constraining human behaviour, the BVN employs biometric technology to bypass certain user behaviour. For example, enrolment on the BVN would ensure that users are unable to access their accounts unless they are physically present at ATMs or points of sale. Therefore, the biometric technology undermines the authentication value of PINs and passwords and nullifies the effects of sharing such information with family or friends.[151] However, precisely because of their capacity to compel obedience, self-executing technologies are considered controversial. They therefore raise further questions about legitimacy and choice as well as legal regulation.

6.4.3.1 Are "Lock-in" Technologies Legitimate?

Lock-in technologies are referred to as 'techno-regulation' by Brownsword,[152] and described as the deliberate employment of technology to regulate human behaviour by Lennes.[153] Jaap koops defines them more aptly as 'technology with intentionally built-in mechanisms to

---

[149] Andrew L Shapiro, *The Control revolution How the Internet is putting Inndividuals in charge and Changing the World we Know* (Century Foundation 1999) 161.
[150] See Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (2011) 3 <https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.>accessed 09/10/2014.
[151] See (n 142).
[152] Roger Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25(1) Legal Studies The Journal of Society of Legal Scholars 1, 3.
[153] R.E Lennes, Harde Lessen: Apologie Van Technologie als Regulerings Instrument (Universiteit van Tilburg, Tilburg 2010) 21 cited in Ronald Leenes, 'Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology' (2010) Tilburg Law School Legal Studies Research Paper Series No. 10/2012, 149.

influence people's behaviour'.[154] In his analysis of techno-regulation, Brownsword argues that there are moral and ethical implications of design-based technologies aimed at controlling harm-generating behaviour. Such technologies, he argues, function in ways which override human choice, freewill, and dignity. According to Brownsword, human dignity implies that people should be able to choose not only the right actions but also the wrong ones. Accordingly, because design-based technologies impose behavioural constraints on the subjects, they deprive such subjects of the opportunity to choose between right and wrong. [155]

As Yeung also argues, although a distinction may be made between design-based approaches which operate directly on the individuals decision-making process and those which seek to restrict opportunities for the exercise of individual judgement without overriding their judgements altogether, concerns that the technologies may generally jeopardise constitutional values are legitimate. As she argues, it may lead to a loss of opportunity to appeal to the discretion and judgement of enforcement officials against the inappropriateness or unfair application of regulatory standards.[156] Following the same line of argument, Koops opines that design-based technologies nevertheless raise these concerns even where they are incorporated to enforce legal norms. As he observes;

> …but also if technology is used 'only' to enforce existing legal norms, its acceptability can be questioned since the reduction of 'ought' or 'ought not' to 'can' or 'cannot' threatens the flexibility of human interpretation of norms that are fundamental elements of law in practice.[157]

The above arguments would be correct to the extent that they identify the corrosive effects of design-based technologies on legitimacy and accountability. However, if the arguments were intended to suggest that lock-in technologies reduce users to robotic recipients of industry's inventions, they would be incorrect. To support this point, it is important to note that it is progressive technological modifications that have been used to respond to user

---

[154] Bert Jaap-koops, 'Criteria for Normative Technology: The acceptability of 'Code as Law' in the Light of Democratic and Constitutional Values' in Roger Brownsword and Karen Yeung (eds) *Regulating Technologies, Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008) 158.
[155] Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (n 152) 15-17.
[156] Karen Yeung, 'Towards an Understanding of Regulation by Design' in Brownsword and Yeung, *Regulating Technologies, Legal Futures, Regulatory Frames and Technological Fixes* (n 154) 95.
[157] Jaap-koops, (n 154) 158-159.

problems in payment systems. As examples, by design, mere possession authenticates the use of credit cards, but this creates incentive to steal the card as any holder may use it. To correct this, subsequent ATM cards were designed with an additional requirement for PINs. This means that the user must not only have the card but must know the PIN. There is less incentive to steal this card unless the thief also has access to the PIN. However, the technology also proved susceptible because users wrote PINs on or kept it with the card. To further increase the confidence that the holder of the card is the authorised user, biometric technologies such as fingerprints, iris scan and so on were introduced.[158] Technology is also now being advanced to integrate behavioural biometrics, including typing speed, touch pad dwell time, key selection, and angle of mouse movements, into mobile devices and web applications to build further confidence into authentication processes.[159]

The point made above is that application of behaviour-modifying technology is neither new nor novel. Such technologies have progressively evolved particularly in response to criminal exploitation of payment instruments and processes. This position is correct even if regulatory motivations are unclear or when regulatory intentions are not clearly spelt out. As Murray persuasively argues, the nature of complex regulatory environments often mean regulation may be transparent or opaque. Whether noticeable or not, regulation is justified by the need to protect the regulated entity and others.[160] Also commenting on the notion that user consent creates artificial control, Cate and Mayer-Schonberger rightly contend that consent is not the optimal mechanism to ensure that either information privacy or the free flow of information is being protected because individuals cannot fully grasp the complexity of the situation they are asked to assess.[161] In Koops view, the tendency to ground data protection in informational self-determination leads to consequential focus on user empowerment which is a fundamental fallacy.[162] At best, the requirement for consent gives

---

[158] This example was cited by Lessig, see Lawrence Lessig, *Code Version 2.0* (Basic Books 2006) 41-42.
[159] See eg MasterCard, 'Security Matters Insights on Advancing Security and Fraud Management for Payments Spotlight on Biometrics' (2014) Issue 22; <http://www.mastercard.com/us/wce/PDF/SecurityMatters_2014.pdf>accessed 01/07/2014.
[160] Andrew D Murray, *The Regulation of Cyberspace Control in the Online Environment* (Routledge Cavendish 2007) 23.
[161] Fred H Cate and Viktor Mayer-Schonberger, 'Tomorrow's Privacy Notice and Consent in a world of Big Data' (2013) 3(2) International Data Privacy Law 67, 68.
[162] Bert-Japp Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250, 253.

the users a false sense of self-determination and creates what Schwarz refers to as the "autonomy trap".[163]

Therefore, one may view technologies that lock in or restrict user choices and preferences as a means of protecting the users even from themselves, while at the same time achieving the interests of government and industry in regulating behaviour. In effect, enrolling user biometrics for account authentication or embedding payment cards with fingerprint biometrics as in the proposed BVN will not in itself be illegitimate. The outstanding question is whether there is need for legal control of such activity and how it should be implemented.

6.4.3.2 Accountability and the Law

The examples above demonstrate how technology can be used to bypass certain user behaviour. Although, it was argued that laws cannot directly regulate behaviour, laws play a role by setting the standards of behaviour sought to be locked-in in the first place. In the case of data protection for example, laws have to define what constitutes personal information in order to establish information qualifying for protection. Additionally, legal requirements that the most effective or up-to–date technical safeguard be used may form the basis of integrating biometric technologies into payment instruments and processes. Where laws do not form the basis of such integration as in the case of the BVN in Nigeria,[164] laws would still be required to set the standards of protection for personal information stored in biometric databases. Without such regulation, it is arguable that the risk of fraud arising from data breaches corresponds to the benefits provided by the lock-in technologies. In other words, consumers of the services could be locked-in into a false sense of security if criminals can gain access to identity databases. Arguably, in such circumstances, criminals would have less need of the information which technology protects in the hands of users.

Therefore, in order to address questions of accountability, laws are required to set out evidential requirements to establish that correct security protocols have been implemented into payment instruments or processes that have lock-in effects. A good example here is the Nigerian e-identity card. It was argued in chapter five that because the card is embedded with payment functionalities, it may serve as an access point to payment information by

---

[163] Paul M. Schwatz, 'Privacy and Democacy in Cyberspace' (1999) 52 Verderbilt Law Review 1609, 1659-1662.

[164] The requirement to use biometrics in payments is not backed by any law but is simply an initiative by the CBN to curb e-payment fraud.

multiple organisations which have no need for such information.[165] Conversely, one of the proposed security features of the card is the deployment of firewall technology to separate and protect the financial information on the card.[166] It is therefore possible to argue that unless the protocols used to implement such separation are ascertainable and verifiable, allegations of unauthorised access may be difficult to resolve.

Based on the analysis above and earlier explication of Lessig's theory, cybersecurity for e-payments in Nigeria can be depicted as a process (figure 6.1) in which each regulatory modality affects the others within the regulatory schema.

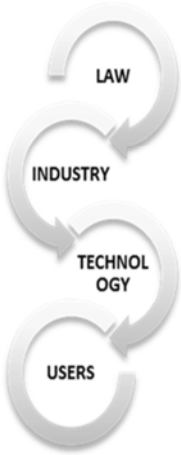

Figure 6.1 Cybersecurity process based on the theory of modalities of control

As shown in *figure 6.1*, law has no direct impact on user behaviour but technology does. Although, technology standards may be translated into legal rules, laws cannot directly regulate technology because technology is evolving and the volatility of technology means security mechanisms become elementary and outdated fairly quickly. However, since industry can readily modify technology, direct regulation of industry by the law would promote the development of high technical standards for data security. To cite few of many possible examples, data protection law may provide that organisations use the most up to date, if not the state of the art in technology to protect personal information. Also, laws regulating electronic payment services may impose liability on providers in certain circumstances where authentication or authorisation is contested. Digital signature laws may allocate higher evidential value to digital against simple electronic signatures. Together, the laws would ensure that the payment industry keeps abreast of developments in criminal skills. It would also ensure that to avoid liability, service providers deploy updated and

---

[165] See notes in 5.1.1 NIMC's Electronic National Identity Card p137.
[166] See eg NIMC, *Facts About the National e-ID Card* <https://www.nimc.gov.ng/?q=facts-about-national-e-id-card>accessed 12/04/2015.

industry recommended technologies including those that may lock-in users in order to comply with legislation.

Conclusion

The analysis in this chapter used Lessig's theory of modalities of regulation to examine the limits of existing legal and regulatory frameworks in the Nigerian e-payment industry. The core of the argument is that law is central to the setting of standards for privacy and security for electronic transactions. Through an examination of the different modalities for controlling e-payment frauds, the arguments demonstrate that the current attempts to curtail cybercrime threats to e-payment systems in Nigeria are inadequate. For example, as the most significant regulatory mechanism in cyberspace, "code as law" may not go far enough because organisations fail to implement it as such. Code may also go further than law and may require legal regulation. While conceding that technology plays a fundamental role in regulation of e-payment frauds therefore, an understanding that technology is malleable and prone to manipulation and abuses underscores the need to regulate industry to regulate technology.

The arguments in the chapter also underline the market economy constraints that undermine any claim of viable industry self-regulation. It was argued that because externalities and information asymmetry affect market efficiency, which is a public good, they also threaten the economy as a whole. By impugning the integrity of payment systems, they heighten the fear of victimisation. The consequences are that users may migrate from arguably more efficient e-payments to less efficient ones such as cash or other paper payments. Invariably, inefficiency precipitates a 'dive to the bottom' and eventual collapse of the payment system and even the economy.

Conversely, laws can foreclose on inefficient self-regulatory schemes and promote user confidence in electronic transactions generally. More significantly, laws can prevent lacunae in the administration of justice by setting clear evidential standards and rules in cases of identity-theft or fraudulent transactions. Overall, a conclusion that self-regulation as an alternative to legal control leaves users mostly unprotected and prone to exploitation is inescapable. Legal regulation is then justified not only on the grounds that law is the most obvious self-conscious agent of regulation, but also on grounds that alternative proposition lead to a replacement of government regulation with a monopolistic self-serving regime of self-regulation.

Chapter Seven

A Proposal for Cybersecurity for E- payment Systems in Nigeria

Introduction

In chapter six of the thesis, arguments were made that self-regulation by the payment industry is inadequate and law is central to achieving effective control of identity-related cybercrimes. It is further argued in this chapter that it is by understanding the functions and limits of different laws that we can better achieve cybersecurity. It is therefore proposed that in formulating cybersecurity for e-payments and indeed cybersecurity generally, policy must take account of the socio- legal factors and the regulatory and enforcement realities of the Nigerian system.

This chapter starts by re-examining the main arguments and findings in the thesis that underpin the proposal. It then evaluates the potentials and limits of criminal and non-criminal laws in the area of controlling identity-related cybercrimes. It is argued in the chapter that because of inherent limitations of criminal legislation and the peculiar challenges of enforcement in Nigeria, policy should promote non-criminal legislation as a means of controlling identity-related cybercrimes. The chapter concludes with specific recommendations for achieving comprehensive cybersecurity in Nigeria. This chapter therefore serves three purposes. One, it highlights the proposal for cybersecurity in e-payments in Nigeria. Two, it advances justifications for the proposal and three, it analyses the factors which make the proposal particularly workable in the Nigerian context.

7.1 Statement of the Proposal

The effectiveness of laws often depends on jurisdictional context. It is therefore important not only to concede to legal regulation but also to identify laws that regulate effectively. In other words, the social context and legal and enforcement regimes in Nigeria require that proposals and implementation for cybersecurity laws be moderated by an understanding of laws that work more effectively. In the context of identity-related cybercrimes in e-payment systems, these are non-criminal legislation aimed at regulating providers of e-payment services. Presently, these laws are being overlooked in favour of criminal legislation. As a result, policy initiatives with respect non-criminal laws on cybersecurity have been comparatively marginal.

The above proposal is underpinned by the empirical data and the theoretical frameworks analysed in this thesis. Three central points can be inferred from the analysis. The first is that because identity-related cybercrimes are pervasive, legal regulation is required to enable industry adequately address the crimes. The second derives from arguments that the social and political challenges of enacting and enforcing a cybercrime law in Nigeria makes it imperative to develop alternative cybersecurity laws. The third point derives from the effectiveness of non-criminal legislation in preventing identity-related cybercrime in the first place. The following sections summarise the main arguments and principal findings in the thesis in order to demonstrate how they lead to the conclusions.

7.2 The Scale of the Problem - Identity-related Cybercrimes are Pervasive

In chapter three, the thesis assessed the pervasiveness of identity-related cybercrimes. The empirical data indicated that it is difficult, if not impossible, to determine the rate of the crime because there are no reliable and evidence based statistics. It was argued that based on the literature and the antecedent of cybercrimes in Nigeria, the lack of statistics cannot be taken as evidence that identity-related cybercrimes are not pervasive.[1] I therefore concluded that it is more logical to attribute the lack of statistics to the "culture of denial" or "culture of secrecy" which implicates unwillingness on the part of organisations to admit the crimes due to reputational concerns.[2]

Further analyses in chapters three, five and six support this point. The arguments demonstrated that in spite of denials of the pervasiveness of the crime, initiatives taken by the Nigerian payment industry suggest a drive towards combatting identity-related cybercrime. For example, concurrent with its denial, industry has also intensified technical responses and education of users on fraudulent activities.[3] The Central Bank of Nigeria's (CBN) biometric verification number (BVN) exercise is an outstanding example in this regard. Therefore, while the culture of denial or culture of secrecy understates the threats, industry's resourcefulness in addressing the threats suggests that the crimes are more widespread than stakeholders are willing to admit. Although, the conclusion (that identity-related cybercrimes are pervasive) appears to be against the weight of the evidence provided by the empirical data, it is also supported by the empirical data and the literature which established that the crimes are indeed pervasive but merely not reported or recorded.

---

[1] See notes in notes in 3.2 The Challenges of Fraud Reporting p 50.
[2] ibid.
[3] See notes in 3.5 Industry Responses to cybercrime Threats –Private Ordering and Technical Security Standards p 73.

7.3 The Challenges of Criminal Legislation

Analyses in chapters two, three, four and five of this thesis established that industry guidelines constitute the principal regulatory instruments for e-payment systems. The theory of modalities of regulation examined in chapter six however demonstrates the standard setting role of the law. When applied to regulation of the Nigerian e-payment system, the theory underlines why it is essential to legislate to regulate e-payment services and institutions. The thesis established that with respect to laws which may control identity-related cybercrimes, progress has been made only at the level of criminal legislation.[4]

The data and documentary evidence, which includes legislative proposals and policy documents, suggest that a criminal law solution drives the debates on cybersecurity in Nigeria. To illustrate this, a total of 18 out of 19 respondents interviewed during the fieldwork proposed criminal legislation as the main solution to cybercrime threats to e-payment systems. This is in contrast to six respondents who specifically mentioned non-criminal regulation such as a data protection law. Furthermore, records of legislative proposals and bill progression indicate that successive cybersecurity bills presented to the Nigerian National Assembly have been lopsided in favour of criminal legislation. More than 15 bills for a cybercrime law have been presented to the two legislative houses at different times. As noted in chapter four, reports suggest that the cybercrime Bill 2014 was signed into law before the expiration of the tenure of the last legislative houses.[5] Comparatively, only one comprehensive proposal for a data protection law was located and even this proposal was not presented to the National Assembly and was never debated. A payment services regulation law proposed in 2009 had lapsed and the records did not indicate that the bill was resuscitated or that a new bill was presented or debated by subsequent legislative houses. No specific proposal for a digital signature law could be located.

It is crucial to restate, as mentioned in chapter four, that in spite of their frequency and consistency, even the proposals for cybercrime law spanned over a period of ten years with some of the bills not even getting a mention by either of the legislative houses. This trend prompted further enquiries into why there were so many bills but none was passed into law.[6] A review of legislative debates failed to give indications of the reasons why the bills were not passed. However, data from the empirical research and further scrutiny of individual bills provided a number of possible explanations. The first explanation is the possibility that

---

[4] See notes in 4.2.3 Hacking Offences under the Cybercrime Bill 2014 p 96.
[5] See (n 47) at p 97.
[6] ibid.

social perceptions of cybercrimes may have contributed to lack of criminal legislation. The second explanation suggests that lack of legislation was due mainly to legislative inaction. The third explanation points to the fact that the passage of a cybercrime law was due to the political "fight for turf" among law enforcement agencies.

7.3.1 Social Perceptions of Cybercrime

The arguments in chapter four may suggest that because of social perceptions of cybercrime, agitation for criminal legislation was not sustained. It was argued for example that society views the crimes as less serious because of the pervasiveness of corruption within the political class. In other words, society tolerates cybercrimes because of perceptions that it leads to lesser financial losses relative to funds embezzled by politicians and other economic criminals. It was also argued that this tolerance of cybercriminals has been documented in the literature and may even be inferred from the popularity of music which extols the exploits of cyber-fraudsters.[7] Although, this research did not undertake a quantitative sampling of the Nigerian population to establish their views of cybercriminals, existing empirical research, and the views of law enforcement agents, lawmakers and policy makers collected during the research demonstrates that such perceptions exist.[8] The explanations of service providers for avoiding liability for fraudulent transactions also demonstrate another crucial perspective on cybercrime. For example, the tendency to argue that hackers are motivated by ideological rather than financial considerations or that users are negligent or collusive suggests that victims of cybercrimes, rather than the criminals are being stigmatised.[9]

It is arguable that the social perceptions of cybercrime are even reflected in law and policy. In chapter four, it was mentioned that rather than establish an enforcement agency for the cybercrime law, the cybercrime bill 2014 proposed a Cybercrime Advisory Council coordinated by the National Security Adviser (NSA). The notable aspect of the provision is that the Council is expected to meet four times a year.[10] It is argued here that the establishment of the council and the prescribed number of meetings suggest a lack of appreciation for the evolving nature of cyber-threats and crimes. What one may ask, could a cybersecurity agency meeting four times a year achieve in the context of fast evolving cyber-threats and cybercrimes? It is therefore possible to conclude that this approach only reinforces society's perceptions that cybercrimes are relatively less serious crimes.

---

[7] See notes in 4.2.3.1 Access without Authority (Basic Hacking Offence) p 97 at 98.
[8] ibid 100.
[9] See eg notes in 6.4.1.3 Security is never "Absolute" p 192.
[10] See generally notes in 4.6.2 The Politics of the "Fight for Turf" p 132.

In view of the many proposals for cybercrime law, and reports that a Cybercrime Act 2015 was eventually passed,[11] the above observations may appear hypothetical. In other words, it is possible to argue that the social perceptions could not inhibit the passage of a cybercrime law. This assessment would be correct. As the arguments in the thesis itself suggest, social perceptions of cybercrimes are more likely to affect the enforcement of the law. It was argued in chapter four that societal perceptions may undermine the prescribed punishment for the basic hacking offence.[12] I argued that as a result of the perceptions, the society, law enforcement and judicial authorities may be inclined to query the jurisprudence and punishment for the basic hacking offence. This is particularly true in view of the fact that the criminal law prescribes arguably less severe punishment for more serious or violent offences. Although, it was noted that the arguments were not intended to exculpate hackers from punishment, I concluded that punishment for the basic hacking offence should be evaluated in the light of the retribution and utilitarian theories of punishment.[13]

In addition to the above, social perceptions may affect reporting systems and therefore the effectiveness of the law. In this regard, the following questions must be raised. One, if cybercrimes are considered as resulting in insignificant financial losses, and victims are adjudged ignorant, negligent, greedy or even collusive in the crime, will they (the victims) bother to report the crimes at all?[14] Two, if cybercrimes reflects on organisations' reputation, will organisations report the crimes? Three, if law enforcement agents view cybercrimes as non-violent and therefore less serious, will they deploy time and resources to reported cases?[15] Finally and more fundamentally, if there are no statistics to show the scale of the crime, will government allocate adequate resources to developing computer forensic capacity for investigation and prosecution of cybercrimes?[16] Negative answers to these questions further underline the argument that criminal legislation on cybercrime would be ineffective.

7.3.2 Legislative Delays

Another explanation for lack of cybercrime legislation is that it is due to inaction on the part of the legislative houses. Although, because of the paucity of debates on the various

---

[11] There is still some uncertainty about the law because of the haste with which the law was purportedly passed; see eg (n 47) at p 97.
[12] See 4.2.3.1 Access without Authority (Basic Hacking Offence) p 97 at 103.
[13] ibid 101.
[14] See notes in 3.4.1 Account Takeover Fraud p 70; see also 6.4.1.3 Security is never "Absolute" p 192.
[15] See particularly (n 62) at p 100.
[16] See 4.6.1 Lack of Computer Forensics Capacity in Law Enforcement p 130.

cybercrime bills sent to the Nigerian National Assembly, this explanation is persuasive, it is not conclusive. It was noted above and earlier in chapter four that numerous proposals have been put forward during the tenure of different legislative sessions. The proposals emanated from different sources including privately sponsored and executive bills. Therefore lawmakers often have to deal with similar proposals from different sponsors almost simultaneously. While this may not justify inaction, it demonstrates that multiple proposals may generate confusion which could delay debates on bills by the legislative houses. It is therefore possible to argue that the sheer volume of legislative proposals on cybercrimes may have considerably slowed down the legislative process.[17]

7.3.3 The "Fight for Turf" Among Law Enforcement Agencies in Nigeria

Perhaps the most persuasive explanation, supported in particular by the data, is that delay in passing the cybercrime law is driven by the battle or fight for turf. It was stated in chapter four that battle or fight for turf represents in-fighting among law enforcement agencies seeking powers to administer or enforce the cybercrime law. As a result, agencies engaged in the turf lobby law and policy makers to abandon proposals which fail to designate them the implementing agency for the cybercrime law.[18] This explanation also finds support in the wordings and provisions of different cybercrime bills. While the bills for cybercrime laws are generally comparable in terms of their scope, they differ on the provisions on enforcement. Subsequent bills either include or expunge provisions relating to the establishment of a cybersecurity agency. To illustrate, a bill proposed to establish a cybersecurity agency which would liaise with relevant law enforcement agencies to enforce cybercrime laws was proposed in 2008. The bill died at the Committee stage.[19] Also, in 2009, a bill titled an 'Act for the establishment of the Nigerian Computer Security and Protection Agency and its Governing Board along the lines of the 2008 bill was proposed.[20] It was unclear whether this bill progressed beyond the first reading.

By 2010, the language of the proposals changed. A bill presented in 2010 to amend the Economic and Financial Crimes Commission (EFCC) Act 2007 sought to confer powers on

---

[17] See particularly (n 46) at p 97.
[18] See notes in 4.6.2 The Politics of the "Fight for Turf" p 132.
[19] See The report of the Joint Committee on Drugs, Narcotics and Financial Crimes, Science and Technology and Justice on A Bill for an Act to provide for the establishment of the Cybersecurity and Information Protection agency charged with the Responsibility to secure Computer Systems and Networks and Liaison with relevant Law enforcement Agency for the enforcement of Cybercrime Laws and Related Matters 2008 [HB 154] Establishment Bill 2008.
[20] See Computer Security and Protection Bill 2009 (HB 321) C 3681.

the EFCC to investigate cybercrimes and e-payment related crimes. By the proposal, the EFCC, which already has the mandate to investigate economic and financial crimes, sought to extend its powers to cybercrimes and e-payment matters.[21] A proposal made in 2011again resuscitated the notion of establishing a cyber-security and information protection agency. The agency is to be charged with the responsibility of securing computer systems network and liaising with the relevant law enforcement agency for the enforcement of cybercrime laws, and for related matters.[22] The bill did not pass legislative approval. The Cybercrime Bill 2014 neither establishes a central cybersecurity nor grants specific powers to any law enforcement agency. As noted in chapter four, this was interpreted to mean there would be no implementing agency for the law. The intent of the law is that all law enforcement agencies in Nigeria develop capacity to investigate and undertake prosecution of cybercrimes.[23]

In addition to the evidence provided by the data therefore, the consistency in the alteration of the provisions relating to the cybersecurity agency suggests that the "fight for turf" among law enforcement agents is the most outstanding factor which delayed criminal legislation on cybercrimes in Nigeria. As the Cybercrime Bill 2014 resolves the problem by refraining from naming any lead or central agency for administration and enforcement of the law, the inference can be drawn that the bill represents a compromise between those in favour of the establishment of an agency and those against it. However, it was argued earlier in chapter four and in the recommendations made later in this chapter that this approach to enforcement is both ineffective and counter-productive.[24]

7.4 Understanding the Limits of Legal and Regulatory Frameworks

I have argued previously that the effectiveness of cybercrime laws would be impeded by social perceptions of the crime. I argue further here that when considered against the factors that inhibit the effectiveness of other forms of cybersecurity laws, the implementation and enforcement challenges of a cybercrime law are almost intractable. The arguments here draw on earlier analysis of relevant provisions of the cybercrime and data protection bills in chapters four and five. The conclusions drawn are summarised below.

---

[21] See Economic and Financial Crimes Commission (Establishment) (Amendment) Bill 2010 (HB 351) C 349.
[22] See Cybersecurity Bill 2011 (HB 154) C4443.
[23] See notes in 4.6.1 Lack of Computer Forensics Capacity in Law Enforcement p 130.
[24] ibid; see also further notes on Creation of Specialised Agency for Cybersecurity below.

7.4.1 Cybercrime Bill 2014- Intractable Challenges of Enforcement and Effectiveness

The analysis of the draft legislation on cybercrime indicated that although the law contains relevant provisions that could aid the control of cybercrimes, the language and scope of the law are generally narrow. Provisions of the bill particularly relevant to identity-related cybercrimes include those on hacking, phishing and identity theft. It was argued that the express criminalisation of unauthorised access in excess of authority addresses the artificial distinctions made between insider and outsider fraud and cybercrime and computer crime by policy and practice in Nigeria.[25] However, an examination of different hacking offences demonstrates that that even when the law is passed, the provisions may produce difficult challenges in terms of enforcement. For example, the arguments suggest that the hacking offences would be more effective if the basic hacking offence is defined in terms of access to data or programs rather than as a strict liability offence. It was also suggested that offenders may escape liability under section 6(2) of the proposed law unless the law is amended to remove the technicality which may arise from the enumeration of further offences.[26] The analysis of the law also led to conclusions that provisions relating to computer fraud and identity theft are still inadequate. The law failed to address questions of ownership of personal information and the crucial question of whether identity information being intangible property is capable of being stolen. [27]

The analysis of the law also identified problems with the enforcement provisions. In this respect, the research data provided the information needed to understand the underlying reasons for decentralising enforcement of the cybercrime law. As already stated above, an important conclusion drawn from the data is that lack of provision for a specialised agency to enforce the law represents a compromise to appease law enforcement agencies engaged in the battle for turf. It was also argued in chapter four that even the proposal to constitute all law enforcement agencies in Nigeria into implementing agencies for the cybercrime law would aggravate the dearth of computer forensic capacity within the Nigerian law enforcement agencies and lead to rivalry which perpetuates the fight for turf.[28] This means in effect that the law recreates the very problem which it was intended to address.

---

[25] See notes in 3.2 The Challenges of Fraud Reporting p 50 at 51; see also notes in 4.2.3.2 Unauthorised Access in Excess of Authority p104 at 105.
[26] See notes in 4.2.3.3 Unauthorised Access with Intent to Obtain Computer Content p 106 at 107.
[27] See 4.5 Identity Theft and Identity Fraud under the Criminal Code Act and the Cybercrime Bill p 123.
[28] See 4.6.2 The Politics of the "Fight for Turf" p 132.

Besides the systemic challenges of enforcement highlighted above, the effectiveness of the criminal law in the area of controlling cybercrimes is generally in doubt. It is trite that the nature of the cyberspace itself interferes with enforcement of the criminal law. Cybercrimes can be transient and are evolving, and offences may be committed across several 'invisible' national borders. These factors make investigation, arrest and prosecution difficult. Correspondingly, since states have different levels of technological development and different enforcement capacities as well as different social and political ethos, harmonisation of laws is both impractical and undesirable. As a consequence, and in spite of agreements and treaties on international cooperation in the area of cybercrime, criminal laws have yielded only marginal results in terms of prosecutions and convictions. The McKinnon's case cited earlier in chapter three provides some support for this position.[29] It has therefore been rightly observed that the threat of punishment has had no significant impact on the prevention of cybercrime. [30] Instructively, Gragido et al capture the near impotence of the criminal law in context of cybercrimes when they observed as follows:

> If you commit a cybercrime, there's almost no chance you're going to be caught. If you are caught, there's almost no chance you're going to be prosecuted. If you are prosecuted, there's almost no chance you're going to be convicted. If you are convicted, there's almost no chance you'll serve the full sentence.[31]

The foregoing observation suggests that in practical terms, cybercrime law has inherent challenges of effectiveness. In other words, absent the peculiar political and enforcement challenges within the Nigerian system, criminal legislation is still unlikely to significantly reduce cybercrimes. Therefore, a cybercrime law could easily become a cosmetic or symbolic law aimed at improving Nigeria's national image before the committee of nations rather than one geared towards effectively fighting the crime.

7.4.2 Regulation of Data Processing- The Privacy and Data Protection Bill 2013

With the aid of the research data, the arguments in chapter three demonstrate that for the same reasons that organisations do not report fraud, they would also not report breaches of data. The main reason already stated above is the culture of denial or secrecy driven by reputational concerns. Therefore, the lack of data breach reports cannot be taken as lack of data breaches in the Nigerian e-payment industry. The analyses in chapter five underline the

---

[29] See 4.2.3.1 Access without Authority (Basic Hacking Offence) p 97 at 98.
[30] See eg Stefan Fafinski, *Computer Misuse Response, Regulation and the Law* (Willan Publishing 2009) 45-95.
[31] Will Gragido et al, *Blackhatonomics an Inside Look at the Economics of Cybercrime* (Elsevier 2012) 4.

relevance of data protection to e-payment systems. It was argued that although individuals could be targets of cybercriminals, organisations' databases are more susceptible and attractive targets because of the volume of identity information they hold. The analysis concluded that industry guidelines on data protection in the telecom and banking industry are incomprehensive and inadequate to protect consumers' personal information.

The examination of relevant provisions of the draft data protection law 2013 suggests possible lacunae and interpretation problems in the law. It was argued in particular that to ensure legal clarity, regulatory certainty and general effectiveness of a data protection law, the law should adopt a risk of harm based approach to defining personal information. This approach contrasts with the expansionist approach taken by the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and the EU law. The arguments therefore underlined the relativeness of laws, and the danger of transposing laws from one jurisdiction to another without due considerations for local or jurisdictional context. As noted in chapter five, the draft law is modelled on the PIPEDA 2000. The PIPEDA itself was modelled on the Canadian Standards Association (CSA) Model Code for Protection of Personal Information developed by business and consumer groups. Consequently, the PIPEDA has been described as a voluntary industry standard which found its way, unusually into the text of legislation.[32]

Data from the research provided further understanding of the challenges associated with regulatory laws such as data protection. Analysis of the data suggests that the payment industry has certain incorrect perceptions of the objective of a data protection law and the obligations of organisations under such a law. As I argued in chapter five, the position of service providers appears to be that users' privacy behaviour could undermine any legal obligation to protect personal information.[33] It was implied that a data protection law has not formed part of active proposals for cybersecurity because certain interests lobby against it. The data also suggested that industry stakeholders particularly regulators and service providers regard a data protection law as 'over-regulation' and as such may form part of this lobby interest. Consequently, I concluded that lack of administrative and enforcement powers under the draft law are attributable to a need to appease the lobby interests. Although, this was not clearly established, it is also possible to infer that industry lobby may

---

[32] see Bill C-12: An Act to Amend the Personal Information Protection and Electronic Documents Act 19 October 2011; see also *Englander v Telus* (2004) 247 D.L.R (4th) 275, [46] where the Canadian Federal Court of Appeal referred to the 'non-legal drafting' of the law.

[33] See notes in (a) Personal information is all Information - Why not the Expansionist Approach? p 153 particularly at 154.

largely account for lack of legislative proposals on digital signatures and regulation of payment services.

The data suggested further that pervasive culture of non-compliance and problems of identity management constitute major challenges to an effective data protection regime in Nigeria. For example, policy objective to develop central systems for unique identification have been unrealisable because of the proliferation of identity management in the private sector and parallel identity programs in the public sector.[34]Although, the challenges posed by systemic non-compliance were not underplayed, it was noted that because the draft law proposes to exclude data processing by the public sector, it promotes inequity and invariably non-compliance.[35]

7.4.3 Laws that Regulate (effectively) Criminal (Reactive) Law vs Non-Criminal Legislation

In order to justify the proposal made at the start of this chapter, it is necessary to restate that in spite of the challenges of cybercrime law, policy in Nigeria appeared to have focused almost exclusively on criminal legislation. However, a number of inferences drawn from juxtaposing the challenges of a data protection regime against those of criminal legislation shows that this approach is inefficient.

Considered from the perspective of passing a law, it is arguable that a data protection law could pass legislative debate quicker. As the research data suggests, similar to the cybercrime law, enforcement provisions in the draft data protection law may have been influenced by lobby or vested interests.[36] However, in contrast to the political fight for turf, "lobbying" against regulation should be considered a legitimate industry reaction. In other words, regulation ordinarily implies burden and no one likes to be burdened, therefore, the overriding consideration for government should be that its duty to protect its citizens outweighs industry interests to avoid regulation.

Also, if viewed from the perspectives of effectiveness and efficiency of the law, regulatory laws such as a data protection law would be more effective because they are preventive. While criminal laws are essentially reactive, and may therefore signify the failure of regulation in the first place, preventive legislation is anticipatory, and has distinctive advantages in the area of crime prevention. Arguably, legislation that regulates to prevent crimes means that Nigeria ends up with smaller percentage of cybercrimes. Consequently,

---

[34] See notes in 5.4.3 Challenges of Identity Management p 169.
[35] See 5.4.2 Non-compliance with Regulation- 'The Culture of Impunity' p 167.
[36] ibid 168.

less use will be made of the criminal law and less burden placed on the penal system. There would also be less demand for the unavailable forensic expertise in law enforcement as is presently the case in Nigeria. Also, following the regulatory scheme in chapter six,[37] the cumulative effect of regulatory laws will raise the stakes for service providers. If they must comply with the laws, they have to develop technologies which make hacking, theft and privacy compromise difficult, if not impossible. In this way, the law invariably aids the development of technology and boosts confidence in e-payments and e-commerce which are the goals of policy in Nigeria.

In addition to encouraging technological innovation and development, laws that prevent criminal access to information systems can also lead to cost savings for the government and users. For example, the regulatory schema in chapter six places the burden of regulation on industry. This is a rational approach however it is viewed. Firstly, industry is better positioned to bear such burden in terms of cost and expertise. Secondly, industry introduced e-payment systems, presumably for users' convenience, but arguably also to save cost and increase business profitability. It is therefore correspondingly reasonable to make industry bear the legal, technical and other incidental costs of securing the payment systems. Since imposing regulatory burdens on industry also implicate the development and implementation of appropriate technologies by industry, this translates into cost savings in the areas of crime control and losses to fraud for government and users respectively. One could argue further that by implementing regulation on data protection and similar laws, government could generate income through fees and regulatory fines imposed for non-compliance. Therefore, because similar to other policy objectives, cybersecurity must compete for the allocation of resources, a shift to proactive legal measures that prevent cybercrimes ensure the achievement of cybersecurity at optimal cost. [38]

With respect to the challenges of non-compliance with regulation, it would be correct to say that whether or not there is a culture of non-compliance, non-compliance must be considered a real risk of any legislative framework. Depending on the system and the subject of regulation, the risks may be marginal or significant. Therefore, the correct approach is for policy to access the risks and then determine whether realistic thresholds for compliance and non-compliance could be set and are acceptable.[39] Without undertaking this

---

[37] See Figure 6.1 p 213.
[38] For example in addition to cybercrimes, policy must also prioritise resource allocation to terrorism and general insecurity which Nigeria presently contends with.
[39] See notes on Regulatory Impact Assessment below.

assessment, it could be deemed irresponsive of government to refrain from regulating activities clearly in need of regulation simply because it anticipates non-compliance.

Furthermore, arguments in chapter six demonstrate that apart from preventing the crimes, if identity theft and fraud do occur, non-criminal laws provide certainty on the allocation of liability to further imbue trust in e-transactions. Infact, it was noted in chapter four that some offences under the proposed cybercrime law such as access in excess of authority would be effective only if supplemented by statutory provisions to report breaches under a data protection regime.[40] Therefore, whether they are meant to deal with acceptance and trust issues,[41] or with security threats or crimes, or with consequential liability problems, non-criminal laws provide the needed scope for regulation.

Finally, it is arguable that unlike cybercrime laws, data protection laws could be more easily enforced nationally and even internationally. For example, organisations which would be target of regulation can be identified by national regulators. Also, drafted correctly, the data protection law could be made to have extra-territorial effect. The EU Data Protection law is a good example in this respect. The law requires that third countries have adequate levels of data protection as a condition for transfer of European origin data to such countries. Therefore, without direct enforcement, the law imposes its own standard of data protection on third countries.[42]

It is important to state however that the intention here is not to argue that criminal legislation is completely irrelevant. Invariably, crimes would be committed and the criminal law would be needed to punish offenders. Indeed as Lord Colville aptly observed;

> The analogy must be with the household and the burglar. We do not wish to suggest to the householder that he must take precautions to make his house absolutely impregnable to a burglar, because we all know that that is impossible.[43]

The objective here is to demonstrate that criminal legislation is not a standalone solution even to cybercrime problems. Therefore, rather than focus on the cybercrime law in a way which suggests that it synonymous with cybersecurity, policy in Nigeria must consider it only as part of a composite framework for cybersecurity. In this thesis, I have argued that

---

[40] See notes in 4.2.3.2 Unauthorised Access in Excess of Authority p 104 at 106.
[41] See notes in 2.4.4 Developing E-commerce p 43 at 45.
[42] See Directive 95/46/EC art 25.
[43] Viscount Colville, 'Computer Misuse Bill [HL] (1989/90) 230, 233.

the effectiveness of data security or technical based security measures is inherently limited. In addition to misuse by industry, data security measures also have the propensity to fail. I have also argued that industry is incapable of effecting composite cybersecurity because industry private ordering systems such as the PCIDSS are not uniformly applied and enforced. More significantly, I conceded to arguments that private ordering systems pre-empt legal regulation and may represent an attempt to exclude such regulation.[44] I concluded that following Lessig's modalities of control, only a mix of the regulatory modalities backed by the force of law would ensure composite cybersecurity. The approach to cybersecurity proposed above would therefore be consistent with the definitions and mechanisms expected to be deployed to achieve cybersecurity.[45]

7.5 Recommendations for Achieving Cybersecurity in E-payment Systems in Nigeria

In this section, I propose, in more specific terms, the solutions required to effect cybersecurity in e-payment systems in Nigeria. The recommendations made here are based on the evaluation of gaps in law, policy and enforcement in the area of cybersecurity in Nigeria. I demonstrate through the analysis that the arguments above can be streamlined into clear and practical recommendations which are also applicable to cybersecurity in its broader scope.

The recommendations are highlighted as follows:

(1) Passing cybersecurity laws that impact on payment service regulation and prevention of identity-related cybercrimes
(2) Setting up specialised and regulatory agencies to implement cybersecurity laws
(3) Developing capacity in the area of cybersecurity
(4) Harmonising identity management programs to make identity management more effective
(5) Incorporating regulatory impact assessment into decision making processes of government.
(6) Ensuring the effective Implementation of National Cybersecurity Strategy through understanding Private/ Public Partnership as an advantage with a Caveat
(7) Engaging in education and public awareness programs on a larger and more extensive scale

[44] See notes in 6.4.1.1 Technology is Expensive p 189 at 190.
[45] See notes in (d)Public Key Infrastructure (PKI) p 82 at 85.

7.5.1 Enactment of Cybersecurity Laws for Electronic Transactions

It is trite that legislation is generally imperfect. However as demonstrated in chapters five and six of this thesis, laws are fundamental for setting and enforcing security standard for e-transactions. This is borne out by the fact that when used appropriately, laws as command-and-control regulation can provide clarity, certainty, and predictability. It allows both the general public and the regulated institutions to know what is required and determine whether it is being achieved.[46]Furthermore, laws contain provisions for sanctions. Since punishment is expensive and has implications for the cost of doing business, businesses are more likely to comply with laws. Laws can therefore establish clear penalty regimes unlike standards such as the PCIDSS where this is unclear. The analyses in chapters two, three and five inidicate that legislation is required to regulate data processing, digital signature and payment systems.

7.5.1.1 Regulating Data Processing

Chapter five of this thesis considered the relevance of data protection law to the prevention of identity related cybercrimes. It is important to summarise here the specific reasons which make the law imperative in Nigeria. Data protection is about social and legal responsibility of the government. This encapsulates protection from crime and exploitation. As an example, the analyses of the cybercrime threats in chapter three demonstrate that if criminals gain access to proprietary systems operated by banks or other payment or even non-payment service providers, the resulting data breach could lead to large scale identity fraud which puts more citizens at risk. Government's role in this aspect is to minimise the possibilities of such large scale compromise through regulation of data processing which would include principles for security and safeguard of personal information.

Apart from fraud prevention, government also needs to protect fundamental rights of privacy and dignity which are undermined by information systems. To illustrate, due to the imperatives of the digital economy, and perhaps on account of cultural perceptions on privacy,[47] Nigerians have not opposed large scale processing of personal data such as the NIMC's national electronic identity card.[48] It is arguable that without mandating legal standards for data protection, these activities would also amount to exploitation. In other

---

[46] OECD, 'Reducing the Risk of Policy Failure: Challenges for Regulatory Compliance' (OECD 2000) 21 <http://www.oecd.org/gov/regulatory-policy/46466287.pdf>accessed 10/04/2015.

[47] See notes in (a)Personal information is all Information - Why not the Expansionist Approach? p 153 at 154.

[48] Compare in this respect the fact that the UK abonded its identity card project over privacy concerns. See eg Identity Documents Act 2010 which repealed Identity Cards Act 2006.

words, if conventional notions of privacy, such as those contained in the Nigerian constitution are effectively dead,[49] then lack of legal protection for personal information must be taken as indicating that the government, its agencies and private institutions have capitalised on a people's willingness to trade their personal information for the necessity of transactions. [50] Conversely, a data protection law would represent government's corresponding obligation to ensure that processing agencies do not misuse the information they collect from citizens and that they protect users' privacy and dignity.

Additionally, as analysis in chapter two of the thesis indicate, new payment systems, institutions and services have developed in Nigeria since policy introduced and mandated the use of e-payment systems. In the case of data protection, this translates into a lack of uniform standard for protection of personal information in respective sectors engaged in or connected with the provision of e-payments. For example, different sets of incomprehensive industry guidelines regulate providers of telecom and banking/financial services and it is still unclear what data protection laws would regulate emerging online payment service providers. The appropriate approach therefore is to pass a general or omnibus data protection law which has the potential to foster uniformity and standardisation. Notably, a general law does not exclude respective sectors from formulating additional guidelines on data processing, provided such guidelines conform to the standards in the law or set higher standards.[51]

Moreover, it is arguable that due to increasing population online and the mobility facilitated by technological development, a data protection law is imperative for Nigeria. According to Greenleaf for example, apart from its global influence, a country's population is also a basis for enacting a data protection law. [52] Statistics have shown that Nigeria has the highest population of internet users in Africa.[53] Therefore, even if statistics also fail to indicate the level of threats to online transactions, a data protection law is fundamental to gaining users' confidence and further integrating Nigeria into the digital economy. As Gillen rightly points out, 'Now instead of debating the nature of the space … [governments] are concerned with

---

[49] See eg Micheal Froomkin, 'The Death of Privacy?' (2000) Stanford Law Review 1461; see also notes in 5.2.1.1 Distinguishing Data protection from Privacy p 141 at 143.
[50] ibid (notes 5.2.1.1)
[51] Graham Greenleaf, 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of convention 108' (2012) 2(2) International Data Privacy Law 68.
[52] ibid.
[53]See Internet world Stats, Internet Users in Africa 2014-Q2<http://www.internetworldstats.com/stats1.htm> accessed 22/02/2015.

controlling access to data and potential for interactions it provides.[54] As a further example, although it was criticised for being anticipatory and pre-emptive,[55] the EU Directive on data protection is now one of the most comprehensive and influential data protection instruments in the world. This demonstrates that even if the perceptions of the risks are low, a data protection law is still a legitimate regulatory instrument in the Nigerian context.

Finally, it is important to restate here that expanding the powers of the regulator and providing for data breach reporting are particularly essential to the effectiveness of a data protection law. For example, by providing regulators with powers to issue large and extensive fines, the law would underline the rationality that the cost of disobedience needs to be set above any possible benefit of non-compliance. With respect to data breach and data notification, I argued in chapter three that organisations fail to report breaches because law and regulation have not distinguished data breaches from general security breaches. I also argued that although the distinction may be highly technical, since there is lack of reporting requirement for data breaches, organisations may justifiably treat data breach as a threat which could be dealt with by organisations' internal security mechanisms.[56] In order to eliminate the technicality therefore, a data protection law must provide that organisations report data breaches regardless of whether they expect consequential fraud to follow such breaches. It is notable in this regard that the US, which has no general legislation on data protection, is proposing to introduce a federal data breach disclosure law.[57] It is also notable that the reform of the European Data Protection Directive includes provisions for mandatory data breach reports.[58]

7.5.1.2 Payment Services Regulation

It was noted in chapter two that to address regulatory challenges in e-payment systems, the Central Bank of Nigeria (CBN) relies on banking legislation and a number of ad hoc

---

[54] Martina Gillen, 'Lawyers and Cyberspace: Seeing the Elephant?' (2012) 9(2) Scripted 131,142.
[55] See eg Paul M Schwartz & Joel R Reidenberg, 'Data Privacy Law: A Study of United States Data Protection (1996) cited in Julia Fromholz, 'The European Union Data Privacy Directive' (2014) 15(1) Berkeley Technology Law Journal 461.
[56] See notes in 3.3.2.1 Hacking (Unauthorised/Illegal Access to computer Systems) p 56 at 58.
[57] See Michael Daniels, 'What You Need to Know about President Obama's New Steps on Cybersecurity' (The White House Blog Jan 14 2015). <https://www.whitehouse.gov/blog/2015/01/14/what-you-need-know-about-president-obama-s-new-steps-cybersecurity> accessed 28/04/2015.
[58] See General Data Protection Regulation, art 31.

guidelines which could potentially create regulatory overlap and conflicts.[59] Therefore, not only is the CBN literally 'biting more than it can chew' in terms of regulation, it is also inhibited by lack of legislation to effectively pursue its regulatory mandate.[60] In terms of regulating the e-payment systems and services and preventing crimes on users and consumers, new laws regulating payment services would create new and more competent regulatory regimes, as well as clear liability rules. The UK Payment Services Regulation (PSR) is a specific example cited in the thesis. The PSR regulates most payment services including electronic fund transfers, banking, market structures, card schemes, software vendors and other ancillary providers. The PSR also appointed the Financial Services Authority (FSA) as the competent authority for its supervision and enforcement. [61]

(it is important to note that while the UK has the laws above, initiatives are now being developed towards a private/public partnership and co-ooperation in the UK. This initiative is not being recommended here because it has not worked in the UK itself. More laws are now being developed progressively to counter threats even when these erode privacy. In Nigeria where compliance is a serious problem and where mechanisms for reporting are unlikely to be used effectively even if they exist and where there is no enforcement capacity, a public/private initiative is unlikely to work)

7.5.1.3 Digital Signature Laws

The arguments in chapter three demonstrated that through the use of certification systems, PKI provides additional security protocol which aids mutual identification and authentication of contracting parties. As the arguments further demonstrate, implementing technical security is a complicated process often beyond the technical skill or knowledge of the average user. Encryption for example may take place independently of a user's knowledge or input as communication is usually between the browser and the web server. As a result, the obligation to encrypt data often falls on organisations handling the data. It was therefore argued that legislation is needed to standardise technical security processes in order to enhance their operations and reliability. Also, applying the arguments relating to the legitimacy and accountability of lock-in technologies in chapter six, the invariable conclusion is that legislation on digital signature translates to law setting standards rather than law qualifying technologies.

---

[59] See notes in 2.3.4.4 Payment Institutions – Institutional Framework for E-Payment Systems in Nigeria p 37.
[60] ibid.
[61] See Payment Services Regulation 2009 SI 2009/209 reg 2.

As I argued further in chapter six, a PKI regime enabled by digital signature laws has far reaching implications for evidence and allocation of liability in cases involving fraudulent or contested e-payments.[62] For example, although the Nigerian Evidence Act admits electronic evidence, the law omits the definitions of different forms of electronic signatures. It also failed to prescribe the weight courts would attach to different forms of electronic signatures or the means by which the correctness of procedures used to generate the signatures may be established.[63] To further illustrate this point, in the case of handwritten signatures, the Evidence Act provides that evidence that a signature is that of a person may be inferred from the fact that a person having the same name, address, business or occupation as the maker of the document is admissible as proof that the document was signed by that person.[64] Correspondingly, the law ought to set out the evidential requirements for e-signatures. This may include how to verify that the correct procedure was used in creating the signature and the means of identifying the signer. This is particularly true with respect to digital signatures which are generated by means of cryptographic algorithms. Presumably, since they are also be supported by certification authorities, the reliability of digital signatures depend largely on the credibility of certification authorities recognised by law.

Therefore, while non-mandatory use of digital signature is consistent with the notion that laws need to be technology neutral, a digital signature law could bridge the gaps identified above. For example, by logical assumption, courts would tend to attach strong evidential value to digital signatures which use a combination of mathematical algorithm and public key cryptosystem to create unique digital fingerprint associated with a person or entity.[65]

7.5.2 Creation of Specialised Agency for Cybersecurity

It was noted previously in chapter four and earlier in this chapter that the cybercrime bill failed to create a central enforcement agency in order to resolve the fight for turf among law enforcement agencies. I argued that this approach to enforcement is ineffective and counterproductive. For the purpose of this recommendation, it is important to demonstrate how this approach would fail to yield the expected results and why it is imperative to create a central agency for cybersecurity.

---

[62] See notes in 6.4.1.2 Technology as Industry Regulation – Misuse in Evidential Matters p190 at 191.
[63] ibid.
[64] See Evidence Act 2011 s 94(1).
[65] See notes in (c) Digital signatures p 81.

In chapter four, it was observed that lack of provision for an implementing agency for the proposed cybercrime law is indicative of expectations that forensic capacity would be developed across all law enforcement authorities in Nigeria. However, it was also argued that an underlying assumption that a blanket power of enforcement to all law enforcement agencies would result in capacity development may also be displaced. As further argued in the chapter, such an approach would lead to a "Jack of all trades" situation, where capacity would exist at mediocre or superficial levels. It was stated that perhaps for similar reasons, the National Assembly contested the proposal to constitute the Office of the National Security Adviser (ONSA) into a "coordinating council" for the implementation of the cybercrime law.[66]

Apart from inhibiting capacity development, a more critical problem with the (decentralised) approach to enforcement is its propensity towards perpetuating the fight for turf. I argued in chapter four that vesting blanket powers on all law enforcement agencies in the area of implementing the cybercrime law could create rivalry which inhibits the sharing of information and intelligence.[67] For example, the rivalry could lead to different agencies carving out 'turf' in respective areas of cybersecurity in a way which further compounds problems of access to and reliability of statistics on cyber-threats and cybercrimes. As specific examples, the Economic and Financial Crimes Commission (EFCC) could claim electronic fraud as its core cybersecurity turf. The National Drug Law Enforcement Agency (NDLEA) may assert authority to investigate online money laundering and terrorist financing. The National Agency for the Prohibition of Trafficking in Persons (NAPTIP) may stake its claim on offences related to online child abuse and so on.[68]

Conversely, if a central agency on cybersecurity exists, all other agencies would be obliged to share information with the central agency. The Economic and Financial Crimes Commission (EFCC) is a good example in this respect. The EFCC was set up mainly to combat economic crimes. This approach makes the EFCC a credible resource on economic crimes in Nigeria. Therefore, if as argued in chapter three, lack of reliable fraud statistics contributes to misunderstandings about the nature and extent of cyber-threats in e-payment systems,[69] then the establishment of a central agency would considerably boost reporting and collation of statistics on cyber-threats and cybercrimes.

---

[66] See 4.6.1 Lack of Computer Forensics Capacity in Law Enforcement p130 at 132.
[67] See 4.6.2 The Politics of the "Fight for Turf" p132 at 133.
[68] See (n 209) at p 131.
[69] See 3.2 The Challenges of Fraud Reporting p 50 at 51.

It is important to state that in setting up a central cybersecurity agency, a more dynamic approach is to create the agency through an establishment Act.[70] This ensures that the agency is not dependent on the passage or otherwise of a cybercrime law.[71] The approach would also separate the narrow notion of cybercrime from the broader concept of cybersecurity. It would side-track ambitious agencies fighting for turf and enable cyber-threats to be accounted for regardless of whether they have been defined as cybercrimes.[72] Consistent with the notion that cybersecurity is not only about cybercrimes and to further de-emphasise 'turf', the agency would be made up of experts in different areas of computer forensics rather than only of personnel drawn from law enforcement. Therefore, a central agency would ensure that Nigeria could coordinate her response to cybersecurity, and develop reliable statistics on cyber-threats to inform policy decisions in the area of cybersecurity. It will also ensure that Nigeria could effectively collaborate with other national and international cybersecurity agencies through the sharing of intelligence on cyber-threats and cybercrimes.

7.5.3 Capacity Development in Computer Forensics

In chapter four, it was noted that stakeholders' have argued that capacity building without cybercrime legislation amounts to wasteful dissipation of resources. The converse position to the effect that laws cannot be effective unless capacity already exists to enforce them was also noted. The arguments in this area therefore tend to oscillate between claims that laws cannot exist in isolation of capacity on the one hand and that there can be no capacity building without legislation on the other hand.[73]

A correct approach here would entail an understanding of the limits that technology places on the law itself. It is trite that on account of the evolving nature of technology and volatility of cyber threats, it would be difficult to achieve a perfect mix of law and expertise at any given time. This is more so given that law generally lags behind developments in technology. If this position is correct, then it is realistic to expect some gaps between laws and achieving the capacity to implement them. In other words, whether laws pre-date or post-date capacity developments, there is likely to always be a gap. This gap would widen in countries like Nigeria where the law has so far not responded. For example, it was mentioned in chapter four that departments already created to ensure control of cybercrimes

---

[70] An example in this respect is the Economic and Financial Crimes Commission (EFCC) Establishment Act 2004 which set up the EFCC.
[71] See further notes on Capacity Development in Computer Forensics below.
[72] See notes in 4.1.1 (Not) Defining Cybercrime p 88.
[73] See notes in 4.6.1 Lack of Computer Forensics Capacity in Law Enforcement p 130.

lack the manpower to carry out meaningful investigations and prosecution of suspected criminals.[74] As there are also no specialised courts for cybercrimes, and no training for judges on the technical aspects of cybercrimes, many cases either do not get to the courts or are tried without reference to the 'cyber' aspect of the crimes.[75]

Based on the above observations, one could contend that arguments as to whether law should precede capacity development or not, have become largely irrelevant. This is not only because capacity is already unwieldy against the crimes, but also because the arguments lay undue emphasis on the implementation of criminal legislation. In other words, the arguments are narrow and incomplete because they fail to take cognisance of the broad scope of cybersecurity and the need to train personnel other than law enforcement agents. It was mentioned previously in this chapter that cybersecurity is not solely about the investigation and prosecution of cybercriminals. Cybersecurity is also about preventing cybercrimes, making information systems resilient, and setting security standards and ensuring conformity with those standards.

Conversely, capacity development on cybersecurity is not limited to law enforcement. For example as with cybercrime investigators, technical expertise will be required for data protection officers. The office of data protection needs to develop expertise to validate protocols put in place by service providers, investigate security breach notifications and discover vulnerabilities as well as to review forensic procedures used by organisations to investigate disputed claims.[76] Consistent with the justifications for data protection and digital signature laws above, capacity development here would strengthen the prevention of identity-related cybercrimes. It would also ensure that well-trained data protection officers could identify threats and vulnerabilities even when organisations fail to detect or report them.

7.5.4 Centralising Identity Management Program

Chapter five identified centralised identity management as crucial to the effective implementation of a data protection regime in Nigeria. The critical argument made in the chapter is to the effect that providers of e-payment and associated services pose substantial risks to users because they collect personal information without legal regulation. It was

---

[74] ibid 131, an example was given of the Computer Crime Prosecution Unit which has not prosecuted any cybercriminal since its creation in 2010.
[75] See eg *Amadi v FRN* discussed at p 113.
[76] See Steven J Murdoch and Ross Anderson, 'Security Protocols and Evidence: Where Many Payment Systems Fail' <http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf> accessed 19/05/2014.

pointed out that the converse is also true as unreliable identification systems undermine the data protection regime. In other words, there must be an effective means of establishing identities for organisations to be confident that they are protecting authentic identity information. The analysis in chapter five also established that although the law vests the management of identities on the Nigeria Identity Management Corporation (NIMC), its objective of developing unique individual identification is undermined by parallel identity management schemes by both public and private organisations. In practice therefore, what exists is a patchwork of identity management systems which compound security problems.[77]

As was further argued in chapter five, apart from concerns about security, multiple identity programs also have implications for cost. Specific examples include the CBN's biometric verification number (BVN) system and the SIM registration exercise by mobile network providers (MNOs). To further illustrate therefore, since the NIMC already collects personal information including the biometrics of all Nigerians, its National identity database should serve as a repository for all public and private organisations for identity verification purposes. It would also appear logical for the CBN and the NCC to simply revert to this database for their respective identification needs rather than commence parallel identity programs. This is more so because the CBN and the NCC are also government institutions and the simultaneous programs must be funded concurrently by the government. Against this background, parallel identity programs not only undermine the mandate and core objective of the NIMC to develop unique identifiers for use offline and online, they are also needless and wasteful. In view of this position, it is crucial to streamline identity management system to free up resources to address security which would be a major concern for the operation of the national identity database.[78]

The process would entail Government revisiting the expected or desired outcomes of identity management and the principles, procedures, laws and policies needed to achieve these outcomes. Specifically, the NIMC Act needs to be amended to map a definitive role for the government in the creation and assurance of unique identities. This would promote confidence in the national e-identity card as an identification system validated by public authority. For organisations, public authority backed unique identifiers gives the assurance that they are protecting genuine and not fictitious or forged or stolen identities. For users, unique identifiers provide assurance that they can be correctly identified and authenticated. For law enforcement, a unique identifier enhances the possibility of correctly identifying

[77] See notes in 5.4.3 Challenges of Identity Management p 169.
[78] ibid.

criminals. Unique identification also helps the government to link individuals to identifiers for access to e-government services.

Conversely, the NIMC itself must be subject to data processing regulations to ensure responsibility and accountability. Accordingly, as argued in chapter five, a situation in which the NIMC could be excluded from regulation under the draft data protection law is unacceptable on legal and ethical grounds.[79] Government also needs to imbue trust in the NIMC identity program and address concerns that it might be another of government's many "white elephant projects".[80] This is particularly true in view of the fact that past identity management programs in Nigeria have failed. For example, the first attempt at identity management commenced in 1979 with the establishment of the Department of National Civil Registration (DNCR) which was assigned the responsibility. Until 2007 when its assets were taken over by the NIMC, the DNCR failed to achieve its objectives. It is therefore concerning that statistics from the NIMC itself indicate that since it commenced enrolment in 2009, it has failed to make the expected progress in terms of the number of people it registers per day. This perhaps account for why government issued a definite, albeit unrealistic, deadline for the completion of enrolment by the end of 2014.[81] However, as suggested below, the proper approach is for government to initiate and sustain awareness mechanisms which imbue trust in the program.[82]

7.5.5 Integration of Regulatory Impact Assessment into Decision Making Process of Government

Regulatory Impact Assessment (RIA) is a decision process aimed at informing political decision makers on whether and how to regulate to achieve public policy goals. It entails the broad analysis of all cost and benefits of a proposed regulatory initiative or of existing regulation.[83] As a systematic evaluation of the potential impacts of government action, RIA asks questions about cost and benefits, the effectiveness of the regulation in achieving policy goals and whether there are superior alternative approaches available to government. The advantages of RIA therefore include cost saving, the ex-ante and ex post evaluation of

---

[79] See 5.4.2 Non-compliance with Regulation- 'The Culture of Impunity' p 167 at 168.
[80] This is used to describe projects which fail to achieve their objectives after considerable investment by government.
[81] Ben Agande, 'Jonathan orders NIMC to Register all Nigerians by Dec, 2014' *Vanguard Newspaper* (Lagos, October 12 2003) <http://www.vanguardngr.com/2013/10/jonathan-orders-nimc-register-nigerians-dec-2014/> accessed 26/02/2014.
[82] See notes on Public Awareness and Education below.
[83] OECD, *Regulatory Cost Assessment Guidance* (OECD Publishing 2014) 9.

regulatory proposals, and the consideration of diverse interests in policy making through wide stakeholders' consultation.[84]

RIA is an important instrument that should be used by the Nigerian government to ensure that legislation meets and continues to be relevant in the context of policy objectives. It is relevant both in the general area of regulation and specific area of regulating technologies. Applied across the broad spectrum of regulation, RIA can be used to address compliance problems in Nigeria. For example, because non-compliance is a systemic problem, RIA can aid the realistic assessment of thresholds for compliance or non-compliance in a specific industry which is to be the target of regulation. This would enable government to determine what initiatives, if any, are required to boost compliance and whether rationales exists for reviewing the cost of disobedience.

In the sphere of digital economy laws, RIA is particularly useful for a number of reasons. Firstly, because of the relative newness of e-payment systems, an evidence based policy instrument like the RIA would aid the collection of evidence such as fraud statistics. This serves to validate the need for regulation and legitimise government action. Secondly, by encouraging consultation among stakeholders, government would identify possible areas of misunderstandings and conflicts. This imbues transparency into decision making process for regulation and has the effect of improving confidence in regulation and promoting voluntary compliance. Thirdly and more importantly, because technology becomes outdated very quickly, RIA would aid the assessment of the effectiveness of laws. This is particularly true because when laws operate in a technology context, they need to be routinely updated in line with the assessment of the threats. This could inform decisions on whether and how to update or amend existing legislation. Therefore, although RIA does not become a substitute for political decision making, its empirical approach makes it a useful tool in the development, review and revision of significant legislation.[85]

7.5.6 Effective Implementation of National Cybersecurity Strategy- Understanding Private/ Public Partnership as an advantage with a Caveat

Policy initiatives to underline the significance of cybersecurity have included the development and implementation of national cybersecurity strategies. [86] A national

---

[84] For a more comprehensive explanation on RIA, see OECD, *Reviews of Regulatory Reform Regulatory Impact Analysis a tool for Policy Coherence* (OECD Publishing 2009).
[85] ibid 12.
[86] See e.g. International Strategy for Cyberspace 2011(USA), Australian Government, Cybersecurity Strategy (2009); Canada's Cybersecurity Strategy 2010 and The UK Cybersecurity Strategy: Protecting and Promoting the UK in a Digital World (Nov. 2011).

cybersecurity strategy is often a policy document outlining the modalities for achieving cybersecurity. Following this trend, the Office of National Security Adviser (ONSA) in Nigeria produced two policy documents referred to as the National Cybersecurity Policy and the National Cybersecurity Strategy.[87] Fundamental aspects of the cybersecurity policy and strategy include recognition of the need to designate certain information infrastructures as critical national infrastructure (CNI) and the procedures for such designation. Other aspects of cybersecurity dealt with include recognising the need for legal frameworks and capacity development in the area of cybersecurity. The strategy further articulated three clear approaches as conditions for successful implementation. These are private/public sector partnership, stakeholders' collaboration and international cooperation.[88]

While the strategy is a positive development in the respects highlighted above, it is arguable that it is still largely a policy document containing vague political statements. To illustrate, it is trite that cybersecurity requires significant resource input on the part of government. However, the strategy omits to demonstrate government's commitment in terms of the cost of implementing or achieving the objectives of the strategy. The commitment of £860 million to the National Cybersecurity Strategy programme over a period of five years in the UK is an example here.[89] A similar approach in Nigeria would enable government to set realistic goals on the means of achieving cybersecurity and on the cost of such achievement. Further aspects of the cybersecurity strategy which suggest lack of commitment to implementation include provisions for review after a period of five years. It is arguable that this provision shows lack of appreciation for the evolving nature of cyber-threats and the urgency of cybersecurity measures. For example, since Nigeria does not currently have regulatory framework on cybersecurity, it would have been reasonable for the policy to set review for a shorter period such as two years. This would enable the ONSA to review the cybersecurity policy and strategy in the light of developments (or lack of developments) in regulatory frameworks. More importantly, as the success of the cybersecurity strategy is

[87] It is not clear why there is a separate policy and strategy document as both appear to have similar objectives and scope. See National Cybersecurity Policy December 2014 <https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf>; see also National Cybersecurity Strategy December 2014 <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIONAL_CYBESECURITY_STRATEGY.pdf> accessed 12/11/2015.

[88] ibid National Cybersecurity Strategy [para 1.1 – 1.6]

[89] This sum appears to have been reviewed upwards to 1.9 billion, see Chancellor's Speech to the GCHQ on Cybersecurity delivered Nov 17, 2015 <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security> accessed 17/11/2015.

hinged on stakeholders' cooperation and information sharing through private/public partnerships (or PPP), it is essential to highlight the problematic aspects of these solutions.

It was noted earlier in this thesis that lack of information sharing among stakeholders on cybercrime and cyber-threats is a major hindrance to understanding the challenges posed by cybercrime and the responses which may be developed. Therefore, cooperation among stakeholders is an essential aspect of cybersecurity. However, while seemingly positive and even simplistic, achieving stakeholders' cooperation poses significant challenges. The problem of international cooperation in the area of cybersecurity particularly as it relates to the legal and social contexts of cybercrimes have been highlighted earlier in this chapter. The arguments will not be repeated here save to reiterate that while international cooperation appear attractive in theory, it is difficult to implement in practice.[90] In fact, it has been noted that to achieve international cooperation in cybersecurity, a nation must agree on international norms of behaviour with like-minded nations.[91]

Private/public partnership (PPP) is another major area which might present a problem. PPP is particularly important because of its increasing relevance in cybersecurity discourse. In the UK, for example, government launched a private/public partnership initiative tagged the Cyber Security Information Sharing Partnership (CISP) in 2013. The CISP delivers a key component of the UK cybersecurity strategy by facilitating the sharing of information on cyber threats in order to make UK businesses more secure in cyberspace.[92] As in the UK, the rationale behind cybersecurity PPP in Nigeria includes the need for wider stakeholders' engagement and information sharing. Specifically, the cybersecurity strategy recognised the position of the private sector as builders, owners and operators of much of the critical information infrastructures (CII) upon which government itself leverage to provide some of its services.[93]PPP is therefore justifiable on the grounds that the private sector itself is potentially the largest economic victim of cybercrime and has much to benefit from information sharing. Furthermore, it is arguable that however expansive its resources, none

[90] See previous notes in 7.4.1 Cybercrime Bill 2014- Intractable Challenges of Enforcement and Effectiveness at 222.
[91] See e.g Chancellor Speech to GCHQ (n 89).
[92] See Press Release, 'Government Launches Information Sharing on Cyber Security' available <www.gov.uk> accessed 09/11/2015.
[93] See National Cybersecurity Strategy 2014 [para 10.2] (n 87)

of the respective stakeholders, whether the private or public sector, could have complete vicinity of the problem of cyber threats if they acted alone.[94]

In spite of its advantages, the problematic aspects of PPP include how to foster trust between the partnering private and public sectors to facilitate information sharing in the first place. It also includes possible conflicts of interests. For example, under an ideal PPP, partners would be required to share information on security breaches and cyber threats and even vulnerabilities. However, it may be impossible to achieve this ideal because private sector organisations are likely to continue to put reputational concerns before their partnership obligations to share information. Also, in practice, organisations are likely to anticipate regulatory reprisals which may lead to adverse publicity and reputational damage even when they share information with the government. It was argued earlier in the thesis that this is the basis on which information sharing among service providers, regulators and law enforcement under the Nigeria Electronic Fraud Forum (NEFF) initiative is bound to fail.[95] On its part, government may refrain from sharing intelligence with the private sector based on considerations of national security, or on grounds that certain information is classified or sensitive. Generally therefore, PPP in the area of cybersecurity would operate under a regime of mutual distrust and suspicion.

Closely related to the issue of trust is how the partnering sectors can avoid conflicts of interests. For example, government's role as a regulator may conflict with its role as a partner. To underline the tendency of PPP to create this conflict, a commentary noted as follows;

> What is the proper way to reconcile –or at least balance- the desire to assure companies that cooperation is beneficial and not an undue risk, while also holding them accountable for deficient security measures or for failing to provide timely and adequate disclosures of cyber vulnerabilities and attacks? The public and private sectors are struggling with that question and legislative efforts have thus far fallen short of providing an adequate answer.[96]

---

[94] See e.g. Press Release, 'Government Launches Information Sharing on Cyber Security' (n 92).
[95] See previous notes in 6.4.2.3 Inability of Industry to meet the Index for Good Regulation 203 particularly at 204.
[96] Judith H Germano, 'Cybersecurity Partnerships: A New Era of Public-Private Collaboration' (2014) Centre on Law and Security New York University Law School, 6 available

Further issues which may give rise to conflicts include claims by private sector organisations that their obligations to protect their users' privacy and other interests conflict with their partnership obligation to share information. More crucially, it can be argued that private sectors may view PPPs as mere political rhetoric or even as patronising since governments can and do implement parallel laws and policies capable of giving them (the governments) mandatory access into private or proprietary information systems. Examples in this respect include the recently passed Cybersecurity Information Sharing Act (CISA) which in the US will serve as the legal basis for mandatory information sharing between the private and public sectors.[97] Also, although limited to data breaches, EU law now proposes to introduce mandatory reporting of security breaches.[98]

It is important to state that the intention here is not to argue that PPP is without merit, or that it should not be used. On the contrary, the foregoing observations are intended to demonstrate that there are significant barriers to overcome if cybersecurity PPP would work effectively in Nigeria. It is therefore recommended here that the proposed PPP should incorporate a number of further elements for effectiveness. Firstly, the PPP must develop modalities for information sharing built on clear guidelines. This may include the development of a code of conduct for information sharing which outlines the rights and obligations of the partners and addresses the privacy interests of users and consumers of private and public sector organisations. Secondly, the PPP must incorporate modalities for developing a high level of trust and incentives for information sharing. For example, the code of conduct may also provide for circumstances where organisations may be exempted from prosecution by customers or users in consequence of information sharing. Thirdly, to ensure accuracy and reliability of information, the partners must develop infrastructure for a virtual collaborative environment so that information can be shared in real time. Finally, while the government and the private sector in Nigeria continue to work on developing trust, the focus of policy should also shift to areas where PPP are more likely to achieve farther-reaching successes. This would include government investment and collaboration in innovation and research which may indirectly facilitate information exchange without the attendant distrust between the partners.

<http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf> accessed 03/11/2015.

[97] See Cybersecurity Information Sharing Act 2015 (US) s 754.

[98] See General Data Protection Regulation, art 31.

7.5.7 Public Awareness and Education

According to the ITU;

> Nigeria does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.[99]

Against the background of the above observation, one must argue that creating public awareness on the nature of the threats online is an important aspect of preventing cybercrimes and promoting cybersecurity. Although service providers already take this approach, the scope of education is narrow relative to the threats.[100] For example, most providers focus on creating awareness information only on in relation to e-mail based phishing scams. However, the growing use of mobile banking and mobile payments also suggests that criminals would migrate to mobile payment platforms. Therefore, in addition to creating awareness about well-known scams, providers should also provide awareness on evolving threats. With respect to mobile payments for example, this would include educating users on how to differentiate between official mobile banking applications and rouge applications, as well as how to check and update payment and banking applications.

On the part of government, broader awareness programs are also required. For example, in addition to the computer emergency response team (CERT) launched in May 2015,[101] government must also sponsor public awareness programs which would further educate users particularly on the significance of registering with the NIMC for identification and verification purposes. Government must also take the lead in creating awareness among service providers on the need for data protection and other regulatory regimes and the legal and social responsibility implicit in the passage of cybersecurity laws.

Conclusion

In this chapter, the clear issues that justify legal interference in cybersecurity initiatives were highlighted and re-examined. The issues include misunderstandings of the nature and extent of cyber-threats as shown by the culture of denial and social and policy perceptions

---

[99] ITU, 'Cyberwellness Profile Nigeria' <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Nigeria.pdf>, 2

[100] See notes in 6.4.3 The Law and Regulation of Users p 205 at 208 .

[101] See https://www.cert.gov.ng/ accessed 28/06/2015.

of cybercrime. They also include politics or political considerations as evidenced by the battle for turf and lack of political will to establish reliable identity management systems.

As a basis for the proposal on cybersecurity in Nigeria, the chapter further summarised the main findings and arguments throughout the thesis. The arguments restate the central role of legislation in ensuring the security for e-payment systems. They also demonstrate that while cybercrime and cybersecurity are global concerns, the imperatives of legislation need to be moderated by an understanding of the limits of respective legal frameworks in the context of different legal systems, societies and cultures. It was argued that on account of the limitations created by the Nigerian social, political and enforcement environment, policy should focus on non-criminal regulation and promote legislation in this area.

While this proposal appears to be against the weight of the evidence which centres on a criminal law based resolution, the arguments made in the chapter provide justifications for the approach. The analysis juxtaposed the peculiar and problematic contexts of both reactive and preventive laws to arrive at the conclusion that proactive laws aid technological developments which prevent identity-related cybercrimes in the first place. The chapter concluded with a list of recommendations needed to achieve the security of e-payments. On account of their scope, the recommendations are also applicable to the broader area of cybersecurity.

Chapter Eight

Conclusion of Central Thesis

8.1 Revisiting the Research Question

As a basis for understanding the challenges of implementing cybersecurity in Nigeria, this thesis set out to examine the legal and regulatory responses to identity-related cybercrimes in e-payment systems. Specifically, the thesis investigated the nature of cybercrime threats to identity information and the reasons underpinning the legal and regulatory responses (or lack of responses) to the threats. The objectives of the research were encapsulated in seven research questions. The central research question formulated by the thesis is, to what extent has the Nigerian law evolved to meet the challenges of cybersecurity in electronic transactions?

In order to place the analysis within the context of e-payment systems, the thesis also formulated ancillary questions as follows; what are e-payment systems and what role do they play in development and governance in Nigeria? How do cybercrimes threaten e-payment systems and how has industry and policy responded to the threats? To what extent has the criminal law responded to the threats of cybercrimes and what reasons account for the response(s) or lack of it? How does the understanding of data protection regimes aid the prevention of identity related cybercrimes and to what extent has the Nigerian law integrated data protection standards? How do theories of cyberspace regulation aid the understanding of the limits of private ordering systems and self-regulation in the context of controlling identity-related crimes in e-payment systems? To aid the development of the electronic economy and considering the context of the Nigerian society and nature of cybercrimes, how should the law best address the challenges of identity related cybercrimes in e-payment systems?

In the following discussion, I summarise the main answers provided in the respective chapters of the thesis.

To set the background for the investigation, chapter one of the thesis highlights the problems and sets the hypothesis. The chapter also identifies the questions sought to be answered and the methodologies used in the research.

In addressing the main research question, the thesis surmised that there are presently no legal measures in place to address the specific problems of cybersecurity. It then examined

this claim by perusal and analysis of policies, laws and regulatory frameworks throughout the thesis. Overall, the research established that although the industry is in denial, and the scale of cybercrime is unascertainable, there is policy awareness of the threats posed by cybercrimes to electronic transactions and to the consumers. However, as analyses in chapters four, five and six demonstrate, Nigerian laws in the areas of cybersecurity have remained largely under-developed. For example, there are no laws regulating providers of electronic services, or laws setting out the liability structure in electronic fraud cases. There are also no data protection laws to protect personal information of consumers and no legislation on cybercrime. The research further revealed that even where proposals for laws have been made, they are mired in political considerations and fraught with interpretational and implementation problems which could render resulting legislation ineffective.

In answer to the central research question, the thesis demonstrated that while policy promotes e-payments and e-transactions, it has failed to develop corresponding legislation to promote trust and confidence in the transactions. Therefore, the laws in Nigeria have not evolved in any significant way to address the challenges of cybersecurity in electronic transactions.

In chapter two, the legal status of e-payments and e-moneys in Nigeria was discussed. It was argued that although they are not currency, e-money and e-payments have analogous functions to currency because they facilitate trade, and function in discharge of monetary obligations once acceptable to the parties involved. It was further argued that to the extent that they perform these functions, e-payments and e-moneys have the same legal effect as currency. Therefore, losses and fraud in e-payment systems are tantamount to loss of money or monetary value. However, it was also argued that because they are not legal tender money, acceptance of e-payments and e-money systems depends largely on the existence of enforceable legal rules and standards which promote users trust and confidence.

The arguments also highlight the fact that increasing internet access and innovations in the payment industry as well as mobility and convenience drives growth of e-payments schemes. Consequently, in addition to traditional payment service providers such as banks, new players have evolved in the payment service industry. However, as the arguments further suggest, because of antecedents of bank failures and consumer confidence problems, acceptance of e-payment in Nigeria have be driven by policy initiatives mandating its use rather by recognition and acceptance by users. The analysis concluded that this development calls for a re-evaluation of laws and regulations relating to financial services.

In order to highlight the significance of e-payment systems to economic and social developments, further analysis in chapter two identified the social and economic advantages of new innovations in payment systems. It was noted that e-payment systems will enhance policy objectives to boost financial inclusion, reduce the cost of cash, improve consumer convenience and develop e-commerce. Although, it was also argued that e-payment systems could lead to reduction in crimes, chapter two concluded that the attendant threats of cybercrime corresponded to the expected benefits of the new e-payment systems.

Chapter three examined the cybercrimes that threaten e-payment systems. The analysis of the concept of identity demonstrated the overlap between real and digital identities and why both forms of identities are relevant to the discourse on cybersecurity. The chapter further analysed hacking, phishing, and malware propagation as the main cyber-threats to e-payment systems. It was noted that hacking considerably threatens proprietary network systems and criminals employ phishing and spamming tactics to exploit both providers and users of e-payment services. However, because of lack of credible and reliable statistics on the scale of the crime, it was argued that the extent of the crime cannot be fully known. The analysis therefore highlights lack of crime statistics as a possible factor contributing to the failure of law and policy to respond to the threats of cybercrimes in Nigeria.

The concluding part of chapter three examined the nature of responses provided by the financial industry to control identity-related crimes. The analysis established that authentication protocols and encryption technology as well as the PCIDSS standards developed by the payment card industry represent the main industry responses to combat the threats of cybercrimes and protect users' personal information. The analysis further established that while these technical measures are admittedly indispensable to the security of the payment systems, their effectiveness is impaired by the growing technical sophistication of criminal attacks and lack of legal frameworks such as those regulating digital signatures.

Chapter four evaluated the criminal law response to the specific cybercrimes identified in chapter three. In order to set the background for the analysis of the law, the chapter examined the state of the Nigerian law on cybercrime. It was noted that there are presently no specific laws which criminalises cybercrime. In order to demonstrate the limits of extant criminal legislation in the area of cybercrimes, the provisions of the Nigerian Criminal laws including the Criminal Code Act and the Advance Fee Fraud Act were examined. It was argued that provisions in the laws relating to trespass and damage to property, as well as to theft, impersonation and fraud were either inapplicable or inadequate to deal with

cybercrimes such as hacking and phishing. The chapter also examined the proposed cybercrime law, the Cybercrime Bill 2014. Possible interpretation challenges of the proposed law were examined with reference to the UK Computer Misuse Act (CMA) 1990. It was argued in particular that the cybercrime bill failed to strike the appropriate balance between certain types of cybercrimes, such as hacking, and the punishment for the crime. The bill also failed to criminalise identity theft. More crucially, the bill failed to make significant improvements in the area of developing the concept of computer-related fraud. Therefore, it still remains a grey area whether a person is criminally liable if he steals personal information by misrepresenting himself to a computer system.

Chapter four concluded with the examination of the enforcement challenges of the proposed cybercrime law. The chapter draws on evidence from the research data to conclude that politics and lobby interests, as well as enforcement challenges contribute significantly to the slow response of criminal legislation on cybercrime in Nigeria.

Chapter five of the thesis examined the regulation of data processing in Nigeria. It was argued that data protection law is a viable legislative instrument for preventing identity related crimes in the multi-stakeholder industry of e-payment services. Chapter five therefore evaluates the concept of data protection. To clarify the nature and functions of data protection relative to privacy, the chapter examined the distinctions between the concepts of privacy and data protection. It was argued that in contrast to privacy, data protection protects specific privacy rights involved when personal data is processed.

Also, in chapter five the guidelines and regulations on data protection in the banking and telecommunications sectors in Nigeria were examined. It was argued that regulation of data processing in the respective sectors is incomprehensive and cannot accommodate the new threats to data processing activities. The examination of the NIMC's e-identity card and NCC's SIM registration as well as the CBN's BVN exercise suggested that there is a need for a more comprehensive and uniform approach to data protection.

Chapter five concluded the analysis on data protection by drawing on the empirical work and the literature. It identified non-compliance and identity management as the main barriers to an effective data protection regime in Nigeria. Therefore, the chapter established that as far as data protection is concerned, the law has not developed sufficiently to address potential threats to personal or identifying information.

In order to demonstrate how the theories of regulation aid an understanding of the limits of self-regulation currently operative in the Nigerian e-payment industry, chapter six evaluates

different theories of regulation of cyberspace. The chapter considered the self-regulatory approach promoted by the cyberlibertarians and concluded that the approach generally falls short of what true regulation entails. After examining the alternative position proposed by the cyberpaternalists, the chapter finds that Lessig's theory of modalities of control built around law, code, market, and norms provides a useful explanation of how regulatory mechanisms which work in real space also apply to the cyberspace. Although, because of the difficulties of formulating widely acceptable normative preferences, it was argued that Lessig's notion of norms be substituted for 'users', the chapter generally concede to the correctness of Lessig's proposal to the effect that regulation by law is central to the effectiveness of other modalities of regulation in cyberspace.

Accordingly, and to justify the position advocated by the theory, the chapter considered the respective limitations of industry, technology and users in controlling crimes in e-payment systems in Nigeria. It was established that technical standards are not wholly efficient because of the volatility of technology, its associated costs and the propensity of industry to manipulate and misuse technical security measures. It was also established that market considerations such as asymmetric information and the operation of negative externalities demonstrate that industry is often motivated by self-interest and is incapable of self-regulation. It was further argued that ability of users is limited by the complexity and cost of technology and even attempts to educate users on the threats online may yield conflicting and unanticipated results. To this end, the chapter concluded that although controlling identity-related cybercrimes entails the broad spectrum of the mechanisms for cybersecurity, law is central and promotes, rather than marginalise non-legal mechanisms of regulation.

In chapter seven, it was argued further that cybersecurity laws need to be carefully and selectively deployed in order to be effective in the context of the Nigerian society. It was proposed that laws which prevent rather than those that react to cybercrimes are likely to be effective in controlling identity-related crimes in e-payment systems. In making the argument, the chapter summarised the main findings in the thesis which underpin the proposal. These include the effects of the social and policy perceptions of cybercrimes on the effectiveness of criminal legislation, and the attendant problems of enforcement due to the battle for turf, as well as lack of capacity for enforcement and the general ineffectiveness of criminal legislation in the area of cybercrime. The arguments demonstrate that a proposal to promote non-criminal legislation is supported by the imperatives of the digital economy, encouraging technological development and achieving policy objectives at minimal cost.

Chapter seven made specific recommendation for achieving cybersecurity in Nigeria. The recommendations suggest that although no legislation is perfect in the sense of achieving all its expected objectives, non-criminal laws minimise the problems and make cybersecurity more achievable. The recommendations also suggest that to achieve cybersecurity, an amalgam of laws rather than one specific law or the other is needed. The chapter therefore concludes by demonstrating how cybersecurity would best be achieved considering the Nigerian social, political and legal contexts.

8.2 Broader Application of Research

It was noted in the introductory chapter to this thesis that a solution to identity-related cybercrimes in e-payment systems has wider implications for the development of appropriate responses to different types of cybercrimes and cyber-threats. These may include the use of the internet for money laundering and terrorist financing. Therefore, since the overall objective of the thesis is to understand the challenges of implementing cybersecurity in Nigeria, the arguments and data generated by the research, as well as the conclusions are transposable to the general area of cybersecurity.

As examples, the data suggests that government should expect denials of the pervasiveness of cybercrime particularly where there are industry and service provider interests at stake. Lobbying from vested interests is also to be expected when regulation is proposed or imminent. Furthermore, because of the technical nature of cybercrime and cybersecurity, government should expect misunderstandings of cyber-threats and their effects. Arguments in this thesis also demonstrate that regardless of the nature of cyber threats and crime, the challenges of enforcement, investigations and prosecution are likely to be the same. The analyses further suggest that because of the interconnection and interdependence enabled by the internet, extant legislation which deals with core services or activities are no longer adequate. Hence, data processing in different sectors including telecommunications, financial services and all e-commerce may be regulated by a common legislation such a data protection law.

Overall, the analyses in the thesis demonstrate that for developing the digital economy, the same regulatory modalities used for real world transactions are applicable and useable. Therefore, a ‘wait and see’ policy approach to regulating emerging technologies is neither necessary nor conventional wisdom. This is particularly true when fundamental interests such as protection of human rights, prevention of crimes and the financial welfare of the nation or even of individuals is at stake.

Bibliography

Abrazhevich D, *Electronic Payment Systems: A User-Centered Perspective and Interaction Design* (Eindhoven 2004)

Adeniran A I, The Internet and the Emergence of the Yahoo-boys Sub-culture in Nigeria (2008) 2(2) International Journal of Cyber Criminology 368

Akerlof G A, 'The Market for "Lemons": Quality Uncertainty and the Market mechanism' (1970) 84(3) The Quarterly Journal of Economics 488

Allen A L, 'An Ethical Duty to Protect One's own Information Privacy' (2014) Alabama Law Review 64(4) 845

Allen A L, 'Privacy-as Data-Control: Conceptual, Practical, and Moral Limits of the Paradigm' (1999-2000) 32 Conn. L. Rev 861

Allen A L, 'What Must We Hide: The Ethics of Privacy and the Ethos of Disclosure' (2012) 25 St. Thomas Law Review 1

Allen W H, 'Computer Forensics' (2005) IEEE Security and Privacy 59

Alvarez M R, and Hall T E, *Electronic Elections: The Perils and Promises of Digital Democracy* (Princeton University Press 2008)

Amfara V A (Jr) and Mertz N T, *Theoretical Frameworks in Qualitative Research* (Sage Publications 2006)

Anderson R, *Security Engineering A Guide to Building dependable Distributed Systems* (2nd edn. Wiley 2008)

Anti-Phishing Working Group (APWG), Phishing Activity Trends Report, Ist Quarter 2012

Anti-Phishing Working Group (APWG), Phishing Activity Trends Report, Ist Quarter 2014

APEC (Asia-Pacific Economic Cooperation) Privacy Framework 2005

Aransiola J.O and Asindemade S.O, 'Understanding Cybercrime Perpetrators and the Strategies they employ in Nigeria' (2011) 14(12) Cyberpsycology, Behaviour and social Networking 759

Article 29 Data Protection Working Party, *Opinion 03/2012 on Purpose Limitation* (WP 203, 2013)

Article 29 Working party *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices* (WP 185, 2011)

Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques* (WP 216, 2014)

Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things* (WP 223 2014).

Article 29 Working Party, *Opinion on the Definition of Consent* (WP 187 2011)

Article 29 Working Party, *Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* (WP 37, 2000)

Article 29 Working Party, *Statement on the Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with regard to the Processing of their Personal Data in the EU* (WP 221 2014)

Austin L M, 'Is consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA' (2006) 56(2) University of Toronto Law Journal 181

Baldwin R, Cave M, and Lodge M, *Understanding Regulation Theory, Strategy and Practice* (2nd edn. OUP 2012)

Barlow J P, 'A Declaration of the Independence of Cyberspace' <https://projects.eff.org/~barlow/Declaration-Final.html> accessed 27/06/2014

Basu S, 'Privacy Protection: A Tale of Two Cultures' (2012) 6(1) Masaryk University Journal of Law and Technology 1

Bazeley P, *Qualitative Data Analysis Practical Strategies* (Sage London 2013)

Becker H, 'Generalising from Case Studies' in Elliot W Eisner and Alan Peshkin (eds), *Qualitative Inquiry in Education: The Continuing Debate* (New York Teachers College Press) 240

Bentham J, An Introduction to the Principles of Morals and Legislation- A New Ed. Corrected by author (Volume 1 London 1823)

Berzins C, 'Three Years under the PIPEDA' (2004) Canadian Journal of Law and Technology 113

Black J, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1

Bollen R, 'A Review of the development and Legal Nature of Payment Facilities' (2005) 16 Journal of Banking and Finance Law and Practice 130

Bond M, et al, 'Chip and PIN: Cloning EMV Cards with the Pre-play Attack' (2012) <http://arxiv.org/pdf/1209.2531v1.pdf> accessed 21/09/2013

Brenner S W, 'Is There Such a Thing as "Virtual Crime" (2001) 4 Cal Crim Law Rev 1

Brownsword R, and Yeung, K, (eds) *Regulating Technologies, Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008) 158

Brownsword R, Code, Control, and Choice: Why East is East and West is West (2..0) 25(1) Legal Studies 1

Bygrave L, 'Privacy and Data Protection in an International Perspective' (2010) Stockholm Institute for Scandinavian Law 165

Bygrave L, 'The Place of Privacy in Data Protection Law' (2001) UNSW Law Journal 24(1) 277

Bygrave L, *Data Protection Law: Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002) 23

Calo R, 'The Boundaries of Privacy Harm' (2010) (2011) 86(1) Indiana Law Journal 1

Cate F H, 'The Failure of Fair Information Practice Principles' (2006) <http://ssrn.com/abstract=1156972> accessed 05/10/2014

Cate F H, and Mayer-Schonberger V, 'Tomorrow's Privacy Notice and consent in a World of Big Data' (2013) 3(2) International Data Privacy Law 67

Cavoukian A, 'Go Beyond Security- Build in Privacy: One Does not Equal the Other (1996) CARDTECH/SECURETECH 96 Conference Atlanta Georgia)

Cavoukian A, 'Privacy by Design: The 7 Foundational Principles' (2011) <https: //www.iab.org/wp content/IAB-uploads/2011/03/fred_carter.pdf> accessed 05/05/2014

Central Bank of Nigeria E-payment Dispute Arbitration Framework 2013 <http://www.cenbank.org/Out/2013/CCD/E-PAYMENT%20DISPUTE%20ARBITRATION%20FRAMEWORK.pdf>accessed 12/05/2014

Central Bank of Nigeria Guidelines on Electronic Banking in Nigeria 2003

Central Bank of Nigeria Guidelines on Point of Sale (POS) Card Acceptance Services 2011

Central Bank of Nigeria Guidelines on stored Value and Pre-paid Card Issuance and Operation 2010

Central Bank of Nigeria Regulatory Framework on Mobile Payment Services in Nigeria 2009

Central Bank of Nigeria Standards and Guidelines on Automated Teller machines (ATM) Operations in Nigeria 2010

Centre for Financial Inclusion, *Glossary of financial Inclusion* http://www.centerforfinancialinclusion.org/page.aspx?pid=1940 assessed 05/03/2012.

Chandler A, 'The Changing Definition and Image of Hackers in Popular Discourse' (1996) 24 International Journal of the Sociology of Law 229

Charmaz K, Constructing Grounded Theory (2nd edn, SAGE 2014)

Charmaz K, *Constructing Grounded Theory, A Practical Guide Through Qualitative Analysis* (SAGE 2006)

Chawki M, ‘Nigeria Tackles Advance Fee Fraud (2009) 1JILT 1
Clarke R, ‘Direct Marketing and Privacy’
<http://www.rogerclarke.com/DV/DirectMkting.html> accessed 21/11/2013
Clough J, ‘Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data’ (2011) 22(1-2) Criminal Law Forum 145
Coffey A, and Atkinson P, *Making Sense of Qualitative Data Complementary Research Strategies* (Sage 1996)
Cohen A I, and Wellman C H, (eds) *Contemporary Debates in Applied Ethics* (Blackwell Publishing 2005) 253
Cohen J E, ‘‘What Privacy is For’ (2013) 126 Harvard law Review 1904, 1919
Cohen J E, *Configuring the Networked Self Law, Code and the Play of Everyday Practice* (Yale University Press 2012)
Cole K et al, ‘Cybersecurity in Africa: An Assessment’ (2008)
http://www.cistp.gatech.edu/publications/files/AnAssessmentofAfricanCybersecurity.pdf accessed 23/08/2012
Council of Europe Global Project on Cybercrime, ‘Cybercrime Strategies Discussion Paper’ (October 2011)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf accessed 23/07/2012
Creswell JW, *Qualitative Inquiry and Research Design Choosing Among Five Approaches* (Sage 2013)
Easterbrook, F H, ‘Cyberspace and the Law of the Horse’ (1996) U. CHI. LEGAL F. 207
EFIna Access to Financial Services in Nigeria Survey 2010 http://www.efina.org.ng/media-centre/news/access-to-financial-services-in-nigeria-survey-2010/ accessed 12/09/2012
El Emam K and Alvarez C, ‘A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques’ (2015) 5(1) International Data Privacy Law 73
European Central Bank (ECB), ‘E-payment Without Frontiers’ (Issue Paper for ECB Conference 10 Nov 2004)
European Central Bank, ‘Glossary of Terms Related to Payment, Clearing and Settlement Systems December 2009
http://www.ecb.int/pub/pdf/other/glossaryrelatedtopaymentclearingandsettlementsystemsen.pdf assessed 19/02/2012
Ezorsky G, *Philosophical Perspectives on Punishment* (Albany: State University of New York Press 1972)
Fafinski S F, Computer Use and Misuse: The Constellation of Control University of Leeds School of Law Thesis September 2008
Fafinski S, *Computer Misuse* (Willan Publishing 2009)
Fafinski S, Dutton W H and Margetts H, ‘Mapping and Measuring Cybercrime’ (2010) OII Forum Discussion Paper No 18
Financial Institutions Training Centre (FITC), Report on Fraud and Forgeries 2012.
Finklea K and Theohary C A, ‘Cybercrime: Conceptual Issues for Congress and the U.S Law Enforcement (2015) Congressional Research Service Report 7-5700
Firestone W A, ‘Alternative Arguments for Generalising From Data as Applied to Qualitative Research (1993) 22(4) Educational Researcher 16
Flick U, *An Introduction to Qualitative Research* (3rd edn. SAGE 2006)
Fried C, ‘Privacy’ (1968) 77 Yale L.J 475, 482
Gercke M, *Understanding Cybercrime: A Guide for Developing Countries* (2nd edn ITU 2011)
Germano J H, ‘Cybersecurity Partnerships: A New Era of Public-Private Collaboration’ (2014) Centre on Law and Security New York University Law School, 6 available

<http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf> accessed 03/11/2015.
Geva B, 'The Concept of Payment Mechanism' (1986) 24 (1) Osgoode Hall L.J 1
Gillen M, Lawyers and Cyberspace: Seeing the Elephant? (2012) 9(2) Scripted 131
Glaser B G, and Strauss A L, *The Discovery of Grounded Theory* (Weidenfield and Nicolson 1967)
Glickman H, 'The Nigerian "419" Advance Fee Scam: Prank or Peril? 39(3)
Goldsmith J, 'Unilateral Regulation of the Internet: A Modest Defence' (2000) 11(1) EJIL 135
Goldsmith, J L, 'Against Cyberanarchy' (1998) 65(4) The University of Chicago Law Review 1199
Goode R, *Commercial Law* (3rd edn, Penguin Books 2004)
Goodhart C and Krueger M, 'The Impact of Technology on Cash Usage' (2001) London School of Economics Discussion Paper 374
Grabosky P N, Virtual Criminality: Old Wine New Bottles? (2001) 10 Social & Legal Studies 243
Grabosky P, Smith RG, and Dempsey G, *Electronic Theft, Unlawful Acquisition in Cyberspace* (Ashgate 2001)
Gragido W, et al *Blackhatonomics An Inside Look at the Economics of Cybercrime* (Elsevier 2012)
Gramlich L, 'Electronic Payments and Electronic Money-Some General Remarks on Factual and Legal Developments' (2008) 2 Masaryk U.J.L & Tech.
Gratton E, 'If Personal Information is Privacy gatekeeper, then Risk of Harm is the Key: A Proposed Method for Determining what Counts as Personal Information (2013) 24(1) Albany Law Journal of Science and Technology 1
Greenleaf G, 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of convention 108' (2012) 2 Int'l Data Privacy L. 68
Hammersley M, *Questioning Qualitative Inquiry: Critical Essays* (Sage 2008)
Hart HLA, *Postscript: Responsibility and Retribution' in Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford: Clarendon 1968)
Home Office Identity Fraud Steering Committee 2006 <http://www.bournemouthcrimeprevention.co.uk/download/printableversion.pdf> accessed 11/08/2012
Humphrey D et al, 'Cost Savings from Electronic Payments and ATMs in Europe' (2003) Federal Reserve Bank of Philadelphia Working Paper 03-16
Information Commissioner's Office (ICO) 'Proposed New EU General Data Protection Regulation: Article- by-Article Analysis Paper' (2013) V1.0
Information Commissioner's Office, Data Protection Act 1998 Legal Guidance Version 1<http://www.valident.co.uk/wp-content/uploads/2012/01/data_protection_act_legal_guidance.pdf > accessed 5/2/2014.
International Engineering Task Force (IETF), 'Network working Group, Request for Comments HTTPS over TLS' http://tools.ietf.org/html/rfc2818 accessed 09/09/2013
International Finance Corporation (IFC), *Mobile Money Summary Report* (2011) http://www.mcit.gov.eg/Upcont/Documents/MobileMoney_09012012.pdf accessed 12/06/2012
International Telecommunication Union (ITU), *Measuring the Information Society 2011* http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf accessed 05/05/2012.
Internet Crime Complaint Centre, *2008 Internet Crime Report*: http://www.ic3.gov/media/annualreport/2008_ic3report accessed 08/05/2012.
Jewkes Y, (ed) *Crime Online* (Willan Publishing 2007)
Johnson D R, and Post D, 'Law and Borders -The Rise of Law in Cyberspace' (1996) 48 STAN. L. REV. 1367

Justice Committee, The *Functions, Powers and Resources of the Information Commissioner* (Ninth Report of session 2012-13 HC 962)

Kang J, 'Information Privacy in Cyberspace Transactions' (1998) 50 (4) Stanford Law Review 1193

Koops B, 'Criteria for Normative Technology The acceptability of 'Code as Law' in the Light of Democratic and Constitutional Values' in Roger Brownsword and Karen Yeung (eds) *Regulating Technologies, Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008)

Koops B, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250

Korff D, 'Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments' (2010) EU Working Paper No.2

Korff D, 'EC Study on Implementation of Data Protection Directive' (2002) Study Contract ETD/2001/B5-3001/A/49

Korff D, 'The Use of the Internet & Related Services, Private Life & Data Protection: Trends & Technologies, Threats & Implications' (2013) Council of EuropeT-PD) 07

Kuan Hon W, Millard C, and Walden I, 'The Problem of 'Personal Data' in Cloud Computing: The Cloud of the Unknowing, Part 2 (2012) 2(1) International Data Privacy Law 3

Kuan Hon W, Millard C, and Walden I, 'The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated? – The Cloud of the Unknowing' (2011) 1(4) International Data Privacy Law 211

Kuner C, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law' (2011) OECD Digital Economy Paper No. 187

Kuner C, *European Data Protection Law* (2nd edn, OUP 2007)

Laidlaw E B, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24(3) International Review of Law, Computers & Technology 263

Landau S, Le Van Gong H, Wilton R, 'Achieving Privacy in Federated Identity Management System' in Dingledine R, and Golle P, (eds) *Financial Cryptography and Data Security* (Springer 2009)

Laudon K C and Guercio T, *E-Commerce 2011 Business Technology Society* (7th edn Pearson 2011)

Law Commission, *Computer Misuse* (WP No 110 1998)

Law Commission, *Criminal Law Computer Misuse* (LAW COM. No. 186, 1989)

Law Commission, *Fraud* (LAW COM No 276 Cm 5560 2002)

Law Commission, *Offences of Dishonest: Money Transfers* (Item 11 of the Sixth Programme of Law Reform1996)

Leenes R, 'Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology' (2012) 5(2) Legisprudence Tilburg Law School Legal Studies Research Paper Series No. 10/2012 143

Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) Harvard Law Review 501

Lessig L, *Code Version 2.0 (Basic Books 2006)*

Levin A, and Nicholson M, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground (2005) University of Ottawa Law and Technology Journal 357

Lindop N, 'Legislating for Data Privacy' in Colin Campell, (ed.) *Data Processing and the Law* (Sweet and Maxwell 1984) 155

Longe O and Osofisan A, 'On the Origin of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers' (2011) 3(1) The African journal of Information Systems

LoPucki LM, 'Human Identification theory and the Identity Theft Problem' (2001-2002) 80 Tex. L. Rev. 89
Makulilo A B, 'Data protection Regimes in Africa, too far from the European 'Adequacy' Standard? (2013) 3(1) International Data privacy Law 42
Makulilo A B, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163.
Mason S and Bohm N, 'Case on Appeal: England and Wales Shojibur Rahman v Barclays Bank PLC case Number 1YE00364 dated 24 October 2012', 175
Mason S, 'Electronic Banking and how Courts Approach the Evidence' (2013) Computer Law and Security Review, Volume 29, Issue 2, 144
Mason S, Electronic Signatures in Law (3rd edn, CUP 2012)
Mayer-Schonberger V, 'Demystifying Lessig' (2008) Wisconsin Law review 713
Metcalfe M, Generalisation Learning across Epitemologies' (2005) 6(1) Forum: Qualitative Social Research available <http://www.qualitative-research.net/index.php/fqs/article/view/525/1136?ref=driverlayer.com/image> accessed 05/11/2015
Microsoft Security Intelligence Report volume 17 2014
Microsoft Security Intelligence Report, Volume 14 2012
Miles M and Hubberman M, *Qualitative Data Analysis: An Expanded Sourcebook* (Sage 1994)
Ministry of Justice, Summary of Responses Calling for Evidence on Proposed Data Protection Legislative Framework Published 28 June 2008, 29 https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/summary-responses-proposed-data-protection-legislation.pdf accessed 23/05//2014
Morse E A, and Raval V, 'PCI DSS: Payment Card Industry Data Security Standards in Context' (2008) 24 Computer Law and Security Report 540
Morse, J M (ed), *Developing Grounded Theory* (Walnut Creek Press 2009)
Murdoch S J, and Anderson R, 'Security Protocols and Evidence: Where Many Payment Systems Fail' http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf accessed 19/05/2014
Murray A D, 'Nodes and Gravity in Virtual Space' (2011) 5(2) Legisprudence 195
Murray A D, *The Regulation of Cyberspace Control in the Online Environment* ((Routledge Cavendish 2007)
Myers S, 'Introduction to Phishing' in Markus Jacobson and Steven Myers (eds), *Phishing and Countermeasures* (Wiley 2007)
Netanel N W, 'Cyberspace Self-Governance: A Sceptical View from Liberal Democratic Theory' (2000) 88(2) California Law Review 395
Newman G R, and Clarke R V, *Superhighway Robbery Preventing e-commerce Crimes* (Routledge 2003)
Nigeria Electronic Fraud Forum (NEFF) Annual report 2012
Nigerian Communication Commission, 'Annual subscriber Data 2001-2014, http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:art-statistics-subscriber-data&catid=65:cat-web-statistics&Itemid=73, accessed 04/12/2014
Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011
Nigerian Communications Commission Consumer Code of Practice Regulations (Federal Republic of Nigeria Official Gazette Vol 84 No 87 of 10th July 2007)
Nigerian National Assembly Debates Fourth Republic Fourth Assembly (Seventh Senate) Fourth Session Senate Official Report (Hansard) vol 1 No 27 of Thursday 23rd October 2014
Nissenbaum H, 'Hackers and the Ontology of Cyberspace' (2004) 6(2) New Media & Society 195

Nwauche E S, 'The Right to Privacy in Nigeria' (2007) 1(1) CALS Review of Nigerian Law and Practice 64

OECD *Reviews of Regulatory Reform Regulatory Impact Analysis A tool for Policy Coherence* (OECD 2009)

OECD, *Anti-spam Toolkit of Recommended Polices and Measures* (OECD Publishing 2006)

OECD, *Online Identity Theft* (OECD Publishing 2009)

OECD, *Policy Guidance on Online Identity Theft* (2008) OECD Ministerial Meeting on the Future of the Internet http://www.oecd.org/sti/consumer/40879136.pdf accessed 12/09/2013

OECD, *Reducing the Risk of Policy Failure: Challenges for Regulatory Compliance* (OECD 2000) <http://www.oecd.org/gov/regulatory-policy/46466287.pdf> accessed 13/04/2015

OECD, *Regulatory Cost Assessment Guidance* (OECD Publishing 2014)

OECD, *Reviews of Regulatory Reform Regulatory Impact Analysis A tool for Policy Coherence* (OECD Publishing 2009)

OECD, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers* (DSTI/ICCP/REG (2008) 10/FINAL

Ogus A, *The Legal Form and Economic Theory of Regulation* (Hart Publishing 2004)

Ogwezzy M C, 'Cybercrime and the Proliferation of Yahoo Addicts in Nigeria' (2012) 1 International Journal of Juridical Sciences 86

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation' (2010) 57 UCLA Law Review 1701

Olinger HN, Britz JJ, Olivier MS, 'Western Cultures and Ubuntu- Influences in the Forthcoming Data Privacy Bill' http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.3533 accessed 03/01/2014

Oriola T, 'Advance Fee Fraud on the Internet: Nigerian Regulatory Response' (2005) 21(3) Computer Law and Security Review 237

Perrit H H, (Jr), 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance' (1998) 5 Indiana Journal of Global Legal Studies 423

Posner R, 'Privacy, Surveillance and the Law' (2008) The university of Chicago Law Review 245

Post D G, 'What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace' (2000) 52(5) Stanford Law Review 1439

Proctor C, *Mann on the Legal Aspects of Money* (6 edn, OUP 2006)

Punch, K F, *Introduction to Social Research: Quantitative and Qualitative Approaches* (2nd edn. SAGE 2005)

R Reidenberg J R, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76(3) Texas Law review 553

Reed C, *Making Law for Cyberspace* (OUP 2012)

Reidenberg J R, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52(5) Stanford Law Review 1315

Reidenberg J R, 'Restoring Americans' Privacy in Electronic Commerce' 14 (1999) Berkeley Technology Law Journal 772

Report of the Committee on Data Protection (Cmnd 7341, 1978)

Rerakyla A and Ruusuvuori J, 'Analysing Talk and Text' in Denzin N K and Lincoln Y S (eds) *The SAGE Handbook of Qualitative Research* (4th edn. SAGE 2011)

Robinson N, and others, 'Review of the European Data Protection directive (2009)(<http://www.rand.org/pubs/technical_reports/TR710.html>accessed 13/05/2014

Rosenberg B, (ed), *Handbook of Financial Cryptography and Security* (Chapman & Hall 2010).

Rotenberg M, 'Fair Information Practices and the Architecture of Privacy' (What Larry Doesn't Get) (2001) Stan Tech L Rev 1

Rubin H J and Rubin I S, *Qualitative Interviewing: The Art of Hearing Data* (2nd edn. SAGE 2005)

Sandler T, *The Theory of Externalities, Public Goods and Club Goods* (CUP 1986)

Sarantakos S, *Social Research* (2nd edn Palgrave 2005) Approaches to Empirical Legal Research' in Cane P and Kritzer HM, *The Oxford Handbook of Empirical Legal Research* (OUP 2010)

Savirimuthu A and Savirimuthu J, 'Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective' (2007) 4(4) Scripted 441-444

Schneier B, *Applied Cryptography: Protocols, Algorithms and Source Code in C* (John Wiley 1996)

Schreft S L, 'Risks of Identity Theft: Can the Market Protect the payment System' (2007) Economic Review Fourth Quarter Federal Reserve Bank of Kansas City Economic Review Fourth Quarterly 5

Schwartz P M and Solove D J, 'Reconciling Personal Information in the United States and European Union' (2013) http://ssrn.com/abstract=2271442 accessed 21/02/2014

Schwartz P M, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices' (2000) Wis. L. Rev. 743

Schwartz P M, 'The EU-U.S. Privacy Collision: A Turn To Institutions and Procedures (2013) 126 Harvard Law Review 1966

Schwartz P M, and Solove D J, 'The PII problem: Privacy and a new Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814

Schwatz P M, 'Privacy and Democracy in Cyberspace' (1999) 52 Verderbilt Law Review 1609

Secretary of State for the Home Department, *Computers and Privacy* (White Paper Cm 6353, 1975)

Seidel J and Kelle U, Different Functions of Coding in the Analysis of Textual Data in Kelle U (ed), *Computer-aided Qualitative Data Analysis: Theory, Methods and Practice* (Sage 1995)

Shapiro A L, *The Control Revolution How the Internet is putting Individuals in charge and Changing the World we Know* (Century Foundation 1999)

Shoeman F D, (ed) *Philosophical Dimensions of Privacy: An Anthology* (CUP 1984)

Simester AP, and others, *Simester and Sullivan's Criminal Law Theory and Doctrine* (Hart Publising 2010)

Simitis S, 'From Market to Polis: The EU Directive on the Protection of Personal Data' (1995) 80 IOWA Law Review 445

Simitis S, 'Revisiting Sensitive Data' Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24-26 November 1999)

Singer M G, 'On Duties to Oneself' (1959) 69(3) Ethics, 202

Smedinghoff T, 'It's All about Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law' (2007) 16(1) Michigan State journal of International Law 1

Solove D J, 'Identity Theft, privacy and the Architecture of Vulnerability' (2002-2003) 54 Hastings Law Journal 1227

Solove D J, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv. L. Rev 1880

South African Law Reform Committee, *Privacy and Data Protection* (Paper 109 2005)

Stefik M, 'Shifting the Possible: How Trusted Systems and Digital Property rights Challenge Us to Rethink Digital Publishing (1997) 12 Berkeley Tech. L.J 137

Symantec Internet Security Threat Report (ISTR) Vol. 17 2012

Symantec Security Report Vol. 17 2012
Tade O and Aliyu I, 'Social Organisation of Internet Fraud among University Undergraduates in Nigeria' (2011) 5(2) IJCC 860
The Law Commission, *Computer Misuse* (WP No. 110 1998)
Thomson J J, 'The Right to Privacy' in Shoeman F D (ed) *Philosophical Dimensions of Privacy: An Anthology* (CUP 1984)
UNODC, Comprehensive Study on Cybercrime Draft, February 2013 <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 23/11/2013.
UNODC, *The Globalisation of Crime; A Transnational Organised Crime Threat Assessment* (UNODC 2010)
Urquhart C, *Grounded Theory for Qualitative Research* (SAGE 2013)
US Cert, 'Computer Forensics' (2008) <https://www.us-cert.gov/sites/default/files/publications/forensics.pdf> accessed 01/04/2015
Uwe Flick, (ed) *The Sage Handbook of Qualitative Data Analysis* (Sage 2014)
Van Hove L , 'Making Electronic Money Legal Tender: Pros and Cons' (2003)Paper Prepared for "Economics for the Future"- Celebrating 100 years of Cambridge Economics, University of Cambridge
Verizon, *2012 Data Breach Investigations Report* http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf accessed 21/09/2014
Verizon, *2015 PCI Compliance Report Insight for Helping Businesses Manage Risk through Payment Security* <http://www.verizonenterprise.com/placeholder/resources/reports/rp_pci-report-2015_en_xg.pdf accessed> 25/03/2015
Wainwright D, 'Can Qualitative Research be Qualitative, Critical and Valid' (1997) 3(2)
Walden I, *Computer Crimes and Digital Investigations* (OUP 2007)
Wall D S, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007)
Warren C A B, 'Qualitative Interviewing' in Gubrium J F and Holstein, J A (eds) *Handbook of Interview Research Context and Method* (SAGE 2001)
Webley L, 'Qualitative Approaches to Empirical Legal Research' in Cane P and Kritzer H M, *The Oxford Handbook of Empirical Legal Research* (Oxford, OUP 2010)
Westin A F, 'Social and Political Dimensions of Privacy' (2003) 59(2) Journal of Social Issues 431
Westin A F, *Privacy and Freedom* (Ătheneum, New York 1967)
Whitman J Q, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale Law Journal 1151
Wolf C and Maxwell W, 'So Close, Yet so Far Apart: The EU and U.S. Visions of New Privacy Framework' (2012) 26 Antitrust 8
World bank/Financial Action Task Force (FATF) *Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (OECD/FATF 2011
Worthley K, Bilz K and Darley J M, 'What's Wrong with Harmless Theories of Punishment' (2004) 79 Chi-Kent L.Rev. 1215
Wu T, 'When Code isn't Law' (2003) 89 Virginia Law Review 101
Wu, T, 'Cyberspace Sovereignty? – The Internet and the International System' (1997) 10(3) Harvard Journal of Law and Technology 647
Yeung K, 'Towards an Understanding of Regulation by Design' in Roger Brownsword and Karen Yeung (eds) *Regulating Technologies, Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008) 95
Zittrain J, *The Future of the Internet: And How to stop it* (2nd edn, Penguin 2009)

Appendix

Sample codes

Topic codes	Emerging/sub codes	Core categories
Electronic payments	Novelty	Acceptance problems
	Uncertainty	Regulatory challenges
	Fraud	culture
	Fear	
	Institutions	
	Development	
	National image	
Fraud	Secrecy	Reporting
	Uncertainty	statistics
	Denial	Culture
	Data	Regulatory challenges
	Expertise	
	Technicality	
	Reputation	
	Responsibility	
	liability	
	Uncertainty	
Regulation	Technicality	Compliance problems
	Denial	Self-regulation
	Enforcement	Regulatory efficiency
	Uniformity	
	Culture	
	Delays	
Legislation	Politics	Legislative Effectiveness
	Compliance	Cultural perceptions
	Technicality	Liability
	Culture	Expertise
	Punishment	
	National security	
	National image	
	Technicality	
	Uncertainty	
Security	Uniformity	Privacy
	data	compliance
	monitoring	Self-regulation
	Technicality	Liability