

Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in Internet Cafes and Suggestions for Appropriate Legislation in Nigeria.

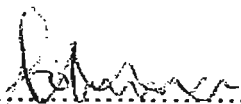
Foluke Oyelayo Laosebikan

Submitted in fulfillment of the requirement for the degree of Doctor of Philosophy (Ph.D), Howard College School of Law, University of Kwazulu-Natal, Durban.

July 2007.

FORMAL DECLARATION

I, Foluke Oyelayo Laosebikan hereby declare that this PhD thesis submitted in the Howard College School of Law, University of Kwazulu-Natal, Durban is my original and independent research. It has not been previously submitted for any degree, and is not being concurrently presented in candidature in any other university. All sources and literature relied on have been duly acknowledged.

Signature 

Date..... July, 2007.....

Supervisor: Prof. D.J. McQuoid-Mason

Signature

Date.....

DEDICATION

To God

For His faithfulness over the years

And for every good and perfect gift;

Especially: Adeyemi Oba, Fehintolu Daniel and Ifeolu Peter.

ACKNOWLEDGEMENT

Heartfelt appreciation and gratitude go to my supervisor, Prof. David J. McQuoid-Mason for his patient supervision and for his graciousness in sharing his depth of knowledge and academic resources in the field of privacy law. Working with him has been a great privilege.

Loving appreciation goes to my husband Dr Adeyemi Laosebikan for encouraging and firmly supporting me throughout this project and for bringing out the best in me always.

I also thank and deeply appreciate Prof & Mrs G.A. Oyedeji (my parents); Dr & Mrs D.A. Laosebikan (my parents-in-law); Dr & Mrs Olusola Oyedeji; Dr & Mrs Adebayo Oyedeji; Mr Adediran Adenugba & Mrs Oluwaseun Adeola Adenugba; Dr & Mrs Olayinka Laosebikan; Mr & Mrs David Monilade Okeniyi, Mr Opeyemi Faramade and Prof & Mrs Opoola Oyedeji for their relentless encouragement and support. I am especially grateful to my sister Oluwaseun, who also took excellent care of the children the many times I needed to be away from home during the course of this work.

I thank and sincerely appreciate Dr Segun Ige, Dr (Mrs) Busayo Ige, Mr Peter Skevington, Mrs Angela Skevington, Dr Goke Akintola and Mrs Bunmi Akintola for their constant encouragement and ready help at every stage of this project. I am also very grateful to Mrs Melanie Richards for her timely immeasurable moral support. In addition, I sincerely thank Mr Karan Naidoo and the Scholarships Office of the Graduate School, University of Kwazulu-Natal, Durban, for their financial support.

Last, but by no means the least, I thank God for the breath of life, His loving sustenance, and the supply of strength and wisdom without which I would not have been able to complete this project.

Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in Internet Cafes and Suggestions for Appropriate Legislation in Nigeria.

Table of Contents

Title Page.....	i
Formal Declaration	ii
Dedication	iii
Acknowledgement	iv
Table of Contents	vi
List of Abbreviations	xxii
Summary.....	xxvi
Chapter One	
<i>Introduction: The Challenge of Information Technology to Privacy</i>	1
1.1 The Right to Privacy	1
1.2 Data Protection	9
1.3 Modern Day Invasion of Privacy	17
1.4 Internet Cafes	22
1.5 The Need for a Re-examination of the Privacy and Data Laws in South Africa and Nigeria	28
1.6 Privacy and Data Protection in South Africa and Nigeria	34
1.7 Conclusion	42
Chapter Two	
<i>The Effect of Information Technology and the Cyber-Revolution on South Africa and Nigeria</i>	43

2.1 Introduction: Evolution and Development of the Computer	43
2.2 Development of Information Technology and its Effects on the Right to Privacy	45
2.2.1 Data Banks and Computerised Pools of Information	
2.2.2 The Internet	
2.2.3 Identity Systems	
2.2.4 Biometrics	
2.2.5 Surveillance Devices	
2.3 Conclusion	62

Chapter Three

<i>Protection of Privacy and Data in the United Kingdom</i>	64
3.1 Introduction.....	64
3.2 Protection of Privacy and Data in the United Kingdom.....	64
3.2. 1 Substantive and Informational Privacy Rights	
3.2.1a Substantive Privacy Rights	
3.2.1b Informational Privacy Rights	
3.2.2 Common Law Protection of Privacy and Data in the United Kingdom	
3.2.2.1 Common Law Protection of Privacy	
3.2.2.1.1 Breach of Confidence	
3.2.2.1.1a Relevance to Internet Cafes	
3.2.2.1.1.1 Breach of Confidence concerning Family Matters	
3.2.2.1.1.1a Relevance to Internet Cafes	
3.2.2.1.1.2 Breach of Confidence concerning Business Matters	
3.2.2.1.1.2a Relevance to Internet Cafes	

3.2.2.1.1.3 Conclusion on the Utility of the English Law of Confidentiality for the Protection of Privacy in Internet Cafes

3.2.2.1.2 Common Law Torts Involving Family and Business

3.2.2.1.2.1 Trespass

3.2.2.1.2.1a Relevance to Internet Cafes

3.2.2.1.2.2 Nuisance

3.2.2.1.2.2a Relevance to Internet Cafes

3.2.2.1.2.3 Defamation

3.2.2.1.2.3a Relevance to Internet Cafes

3.2.2.1.2.4 Malicious Falsehood

3.2.2.1.2.4a Relevance to Internet Cafes

3.2.2.1.2.5 Passing Off

3.2.2.1.2.5a Relevance to Internet Cafes

3.2.2.1.2.6 Intentional Infliction of Emotional Injury

3.2.2.1.2.6a Relevance to Internet Cafes

3.2.2.1.3 Conclusion on Common Law Protection of Privacy in the United Kingdom

3.2.2.2 Common Law Protection of Data in the United Kingdom

3.2.3 Statutory Protection of Privacy and Data in the United Kingdom

3.2.3.1 Statutory Protection of Privacy

3.2.3.1.1 The Human Rights Act

3.2.3.1.1a Relevance of the Human Rights Act to the Protection of Privacy in Internet cafes in Nigeria

3.2.3.1.2 Other Statutes

3.2.3.1.2.1 The Interception of Communications Act

3.2.3.1.2.1a Relevance to Internet Cafes

3.2.3.1.2.2 The 1952 Defamation Act and the 1996

Defamation Act

- 3.2.3.1.2.2a Relevance to Internet Cafes
- 3.2.3.1.2.3 The Protection from Harassment Act
 - 3.2.3.1.2.3a Relevance to Internet Cafes
- 3.2.3.1.2.4 Other Laws Protecting Privacy in the United Kingdom
 - 3.2.3.1.2.4a Relevance to Internet Cafes
- 3.2.3.2 Statutory Protection of Data in the United Kingdom
 - 3.2.3.2.1 The European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data
 - 3.2.3.2.1a Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data
 - 3.2.3.2.1.1 General Data Protection Features of the European Union Directive
 - 3.2.3.2.1.2 Data Protection Principles in the Directive
 - 3.2.3.2.1.3 Liability under the Directive
 - 3.2.3.2.1.4 Relevance to Internet Cafes
 - 3.2.3.2.2 The 1998 Data Protection Act
 - 3.2.3.2.2.1 Definitions
 - 3.2.3.2.2.1.1 Data
 - 3.2.3.2.2.1.1a Annotation
 - 3.2.3.2.2.1.2 Personal Data
 - 3.2.3.2.2.1.2a Annotation
 - 3.2.3.2.2.1.3 Data Subject
 - 3.2.3.2.2.1.3a Annotation
 - 3.2.3.2.2.1.4 Data Controller
 - 3.2.3.2.2.1.4a Annotation
 - 3.2.3.2.2.1.5 Processing

3.2.3.2.2.15a Annotation

3.2.3.2.2.2 Rights of Data Subjects under the Act

3.2.3.2.2.2a Relevance to Internet Cafes

3.2.3.2.2.3 The Data Protection Commissioner

3.2.3.2.2.3a Relevance to Internet Cafes

3.2.3.2.2.4 Data Controllers

3.2.3.2.2.4a Relevance to Internet Cafes

3.2.3.2.2.5 Eight Data Protection Principles

3.2.3.2.2.5a Annotation on the Data Protection Principles

3.2.3.2.2.5b Application to Internet Cafes

3.2.3.2.3 Other Laws Protecting Data in the United Kingdom

3.2.3.2.3.1 The Consumer Credit Act

3.2.3.2.3.2 Access to Medical Reports Act

3.2.3.2.3.3 The Access to Health Records Act

3.2.3.2.3.4 The Official Secrets Act

3.2.3.2.3a Relevance to Internet Cafes

3.3 Conclusion on the Law Protecting Privacy and Data in the United

Kingdom.....177

3.3.1 Privacy Protection

3.3.1a Relevance to Internet Cafes

3.3.2 Data protection

3.3.2a Relevance to Internet Cafes

Chapter Four

<i>Protection of Privacy and Data in the United States of America</i>	184
4.1 Constitutional Protection of Privacy and Data	184
4.1.1 Constitutional Protection of Privacy	
4.1.1.1 First Amendment	
4.1.1.1a Relevance to Internet Cafes	
4.1.1.2 Third Amendment	
4.1.1.2a Relevance to Internet Cafes	
4.1.1.3 Fourth Amendment	
4.1.1.3a Relevance to Internet Cafes	
4.1.1.4 Fifth Amendment	
4.1.1.4a Relevance to Internet Cafes	
4.1.1.5 Ninth Amendment	
4.1.1.5a Relevance to Internet Cafes	
4.1.1.6 Fourteenth Amendment	
4.1.1.6a Relevance to Internet Cafes	
4.1.2 Constitutional Protection of Data in the United States	
4.1.2a Relevance to Internet Cafes	
4.2 Common Law Protection of Privacy and Data in the United States	203
4.2.1 Common Law Protection of Privacy	
4.2.1a Relevance to Internet Cafes	
4.2.2 Common Law Protection of Data	
4.2.2a Relevance to Internet Cafes	
4.3 Statutory Protection of Privacy and Data in the United States	212
4.3.1 Protection of Privacy and Data under Federal Laws	
4.3.1.1 The Privacy Act	
4.3.1.2 Freedom of Information Act	
4.3.1.3 Computer Matching and Privacy Protection Act	
4.3.1.4 Right to Financial Privacy Act	
4.3.1.5 Fair Credit Reporting Act	

4.3.1.6 Electronic Fund Transfer Act	
4.3.1.7 Children's Online Privacy Protection Act	
4.3.1.8 Video Privacy protection Act	
4.3.1.9 Family Educational Rights and Privacy Act	
4.3.1.10 Drivers' privacy Protection Act	
4.3.1.11 Wiretap Act	
4.3.1.12 Electronic Communications Privacy Act	
4.3.1.13 USA PATRIOT Act	
4.3.1.14 Federal Copyright Law	
4.3.2 Protection of Privacy and Data under State Laws	
4.3.2a Relevance to Internet Cafes	
4.4 Conclusion on the Law Protecting Privacy and Data in the United States.....	244
4.4a Relevance to Internet Cafes	

Chapter Five

<i>Protection of Privacy and Data in Germany.....</i>	253
5.1 Constitutional Protection of Privacy and Data.....	253
5.1.1 Constitutional Protection of Privacy	
5.1.1.1 The Right to Self-determination and Protection of Human Dignity	
5.1.1.1a Relevance to Internet Cafes	
5.1.1.2 Privacy of Posts and Telecommunications	
5.1.1.2a Relevance to Internet Cafes	
5.1.1.3 The Inviolability of the Home	
5.1.1.3a Relevance to Internet Cafes	
5.1.2 Conclusion on Constitutional Protection of Privacy in Germany	
5.1.2a Relevance to Internet Cafes	
5.1.3 Constitutional Protection of Data in Germany	
5.1.3a Relevance to Internet Cafes	

5.1.4 Conclusion on Constitutional Protection of Data in Germany	
5.1.4a Relevance to Internet Cafes	
5.2 Civil Law Protection of Privacy and Data in Germany.....	272
5.2. 1 Civil Law Protection of Privacy	
5.2.1a Relevance to Internet Cafes	
5.2.2 Civil Law Protection of Data	
5.2.2a Relevance to Internet Cafes	
5.3 Statutory Protection of Privacy and Data in Germany.....	280
5.3.1 Statutory Protection of Privacy	
5.3.1a Relevance to Internet Cafes	
5.3.2 Statutory Protection of Data	
5.3.2a Relevance to Internet Cafes	
5.3.3 Other Statutes	
5.3.3a Relevance to Internet Cafes	
5. 4 Conclusion on German Law Protection of Privacy and Data.....	291
5.4.1. Conclusion on German Law Protection of Privacy	
5.4.1a Relevance to Internet Cafes	
5.4.2 Conclusion on German Law Protection of Data	
5.4.2a Relevance to Internet Cafes	
Chapter Six	
<i>Common Law Protection of Privacy and Data in South Africa and Nigeria</i>	297
6.1 Common Law Protection of Privacy and Data in South Africa	297
6.1.1 Common Law Protection of Privacy	
6.1.1.1 Wrongfulness	
6.1.1.2 <i>Animus Injuriandi</i> (Intention)	
6.1.1.3 Impairment of Privacy	
6.1.1.4 Relevance to Internet Cafes	
6.1.1.5 Case Law	
6.1.1.5a Relevance to Internet Cafes	

6.1.1.6 Defences

6.1.1.6.1 Defences Negating Unlawfulness

6.1.1.6.1.1 Justification

6.1.1.6.1.1a Relevance to Internet Cafes

6.1.1.6.1.2 Fair Comment

6.1.1.6.1.2a Relevance to Internet Cafes

6.1.1.6.1.3 Necessity

6.1.1.6.1.3a Relevance to Internet Cafes

6.1.1.6.1.4 Consent

6.1.1.6.1.4a Relevance to Internet Cafes

6.1.1.6.1.5 Statutory Authority

6.1.1.6.1.5a Relevance to Internet Cafes

6.1.1.6.1.6 Private Defence

6.1.1.6.1.6a Relevance to Internet Cafes

6.1.1.6.1.7 Absolute Privilege

6.1.1.6.1.7a Relevance to Internet Cafes

6.1.1.6.1.8 Qualified Privilege

6.1.1.6.1.8a Relevance to Internet Cafes

6.1.1.6.2 Defences Excluding Intention

6.1.1.6.2.1 Intoxication

6.1.1.6.2.1a Relevance to Internet Cafes

6.1.1.6.2.2 Insanity

6.1.1.6.2.2a Relevance to Internet Cafes

6.1.1.6.2.3 Mistake

6.1.1.6.2.3a Relevance to Internet Cafes

6.1.1.6.2.4 Jest

6.1.1.6.2.4a Relevance to Internet Cafes

6.1.1.6.2.5 *Rixa*

6.1.1.6.2.5a Relevance to Internet Cafes

6.1.2 Common Law Protection of Data

6.1.2a Relevance to Internet Cafes

6.1.3 Conclusion on Common Law Protection of Privacy and Data in South Africa

6.1.3a Relevance to Internet Cafes

6.2 Common Law Protection of Privacy and Data in Nigeria329

6.2. 1 Common Law Protection of Privacy

6.2.1.1 Breach of Confidence

6.2.1.1a Relevance to Internet Cafes

6.2.1.2 Trespass to Person

6.2.1.2a Relevance to Internet Cafes

6.2.1.3 Trespass to Land

6.2.1.3a Relevance to Internet Cafes

6.2.1.4 Trespass to Chattel/Property

6.2.1.4a Relevance to Internet Cafes

6.2.1.5 Nuisance

6.2.1.5a Relevance to Internet Cafes

6.2.1.6 Defamation

6.2.1.6a Relevance to Internet Cafes

6.2.1.7 Passing- Off

6.2.1.7a Relevance to Internet Cafes

6.2.1.8 Intentional Infliction of Emotional Distress

6.2.1.8a Relevance to Internet Cafes

6.2.2 Common Law Protection of Data in Nigeria

6.2.2.1 Breach of Confidence

6.2.2.1a Relevance to Internet Cafes

6.2.2.2 Trespass to Land

6.2.2.2a Relevance to Internet Cafes

6.2.2.3 Trespass to Property

6.2.2.3a Relevance to Internet Cafes

6.2.2.4 Nuisance

6.2.2.4a Relevance to Internet Cafes

6.2.2.5 Defamation

6.2.2.5a	Relevance to Internet Cafes	
6.2.2.6	Passing Off	
6.2.2.6a	Relevance to Internet Cafes	
6.2.2.7	Intentional Infliction of Emotional Distress	
6.2.2.7a	Relevance to Internet Cafes	
6.2.3	Conclusion on Common Law Protection of Privacy and Data in Nigeria	
6.2.3a	Relevance to Internet Cafes	
6.3	Conclusion on Common Law Protection of Privacy and Data in South Africa and Nigeria.....	348

Chapter Seven

Constitutional and Statute Law Protection of Privacy and Data in South Africa and Nigeria 352

7.1	Statutory Protection of Privacy and Data in South Africa	352
7.1.1	Constitutional Protection	
7.1.1.1	Constitutional Protection of Privacy in South Africa	
7.1.1.1a	Relevance to Internet Cafes	
7.1.1.2	Constitutional Protection of Data in South Africa	
7.1.1.2a	Relevance to Internet Cafes	
7.1.2	Statutory Protection	
7.1.2.1	Statutory Protection of Privacy in South Africa	
7.1.2.1.1	The Promotion of Access to Information Act	
7.1.2.1.1a	Relevance to Internet Cafes	
7.1.2.1.2	The Interception and Monitoring (Prohibition) Act	
7.1.2.1.2a	Relevance to Internet Cafes	
7.1.2.1.3	The Telecommunications Act	
7.1.2.1.3a	Relevance to Internet Cafes	
7.1.2.1.4	The Telegraph Messages Protection Act	
7.1.2.1.4a	Relevance to Internet Cafes	
7.1.2.1.5	The Criminal Procedure Act	

- 7.1.2.1.5a Relevance to Internet Cafes
- 7.1.2.1.6 The Civil Proceedings Evidence Act
 - 7.1.2.1.6a Relevance to Internet Cafes
- 7.1.2.1.7 Natal Law to Amend the Law of Evidence
 - 7.1.2.1.7a Relevance to Internet Cafes
- 7.1.2.1.8 The Copyright Act
 - 7.1.2.1.8a Relevance to Internet Cafes
- 7.1.2.1.9 The National Credit Act
 - 7.1.2.1.9a Relevance to Internet Cafes
- 7.1.2.1.10 The Consumer Protection Bill
 - 7.1.2.1.10a Relevance to Internet Cafes
- 7.1.2.2 Statutory Protection of Data in South Africa
 - 7.1.2.2.1 The Electronic Communications and Transactions Act
 - 7.1.2.2.1a Relevance to Internet Cafes
 - 7.1.2.2.2 The Statistics Act
 - 7.1.2.2.2a Relevance to Internet Cafes
 - 7.1.2.2.3 The Income Tax Act
 - 7.1.2.2.3a Relevance to Internet Cafes
 - 7.1.2.2.4 The Promotion of Access to Information Act
 - 7.1.2.2.4a Relevance to Internet Cafes
 - 7.1.2.2.5 The Criminal Procedure Act
 - 7.1.2.2.5a Relevance to Internet Cafes
 - 7.1.2.2.6 The Regulation of Interception of Communications and Provision of Communication- Related Information Act
 - 7.1.2.2.6a Relevance to Internet Cafes
 - 7.1.2.2.7 The National Credit Act
 - 7.1.2.2.7a Relevance to Internet Cafes
 - 7.1.2.2.8 The Consumer Protection Bill
 - 7.1.2.2.8a Relevance to Internet Cafes
- 7.1.3 Conclusion on Statutory Protection of Privacy and Data in South Africa
 - 7.1.3a Relevance to Internet Cafes

7.2 Statutory Protection of Privacy and Data in Nigeria.....	407
7.2.1 Constitutional Protection	
7.2.1.1 Constitutional Protection of Privacy in Nigeria	
7.2.1.1a Relevance to Internet Cafes	
7.2.1.2 Constitutional Protection of Data in Nigeria	
7.2.1.2a Relevance to Internet Cafes	
7.2.2 Statutory Protection	
7.2.2.1 Statutory Protection of Privacy in Nigeria	
7.2.2.1.1 The Criminal Code Act	
7.2.2.1.1a Relevance to Internet Cafes	
7.2.2.1.2 The Penal Code	
7.2.2.1.2a Relevance to Internet Cafes	
7.2.2.1.3 The Criminal Procedure Act	
7.2.2.1.3a Relevance to Internet Cafes	
7.2.2.1.4 The Evidence Act	
7.2.2.1.4a Relevance to Internet Cafes	
7.2.2.1.5 The Defamatory and Offensive Publications Act	
7.2.2.1.5a Relevance to Internet Cafes	
7.2.2.1.6 The Copyright Act	
7.2.2.1.6a Relevance to Internet Cafes	
7.2.2.1.7 The <i>Sharia</i> Penal Code Law	
7.2.2.1.7a Relevance to Internet Cafes	
7.2.2.2 Statutory Protection of Data in Nigeria	
7.2.2.2.1 The Computer Security and Critical Information Infrastructure Protection Bill	
7.2.2.2.1a Relevance to Internet Cafes	
7.2.2.2.2 The Nigerian Communications Act	
7.2.2.2.2a Relevance to Internet Cafes	
7.2.2.2.3 The Wireless Telegraphy Act	
7.2.2.2.3a Relevance to Internet Cafes	
7.2.2.2.4 The National Population Commission Act	

7.2.2.2.4a Relevance to Internet Cafes

7.2.3 Conclusion on Statutory Protection of Privacy and Data in Nigeria

7.3 Conclusion on the Law Protecting Privacy and Data in South Africa and Nigeria... 432

7.3a Relevance to Internet Cafes

Chapter Eight***Suggestions for the Reform of Privacy and Data Protection Law in Nigeria.....434***

8.1 Suggestions for the Reform of Privacy Law in Nigeria.....434

8.1a Relevance to Internet Cafes

8.2 Suggestions for the Reform of Data Protection Law in Nigeria.....438

8.2a Relevance to Internet Cafes

Chapter Nine***Principles and Provisions for the Protection of Privacy and Data in Internet Cafes in Nigeria.....442***

9.1 Purpose.....442

9.2 Scope.....442

9.3 Liability.....443

9.4 Principles.....445

9.5 Exemptions.....456

9.6 Administration and Enforcement.....458

9.7 Conclusion.....458

Chapter Ten***Summation and Conclusions.....460***

10.1 Overall Summary.....460

10.1.1 United Kingdom

10.1.2 United States of America

10.13 Germany	
10.1.4 South Africa	
10.15 Nigeria	
10.2 Overall Conclusion.....	465

Appendix

Research Methodology	468
1.1 Introduction.....	468
1.2 Setting of the Study.....	470
1.2.1 South Africa	
1.2.2 Nigeria	
1.3 Research Population.....	471
1.4 Data Collection.....	472
1.5 Research Instrument.....	474
1.6 Data Analysis and Findings.....	475
1.6.1 The Questionnaires	
1.6.1a South Africa	
1.6.1b Nigeria	
1.6.2 The Internet Café Interviews	
1.6.2a South Africa	
1.6.2b Nigeria	
1.6.3 The Survey	
1.6.3a South Africa	
1.6.3b Nigeria	
1.7 Validity and Reliability.....	481
1.8 Ethical Issues.....	482
1.9 Difficulties and Observations.....	483
1.10 Conclusion.....	485

Annexure A

Copy of Questionnaire Administered to Internet café Customers.....	487
---	------------

Annexure B

Interview Questions Administered to Internet Café Owners.....489

Annexure C

Questions Asked in the Lecturer/ Student Survey.....490

Bibliography491

Table of Statutes506

Table of Cases515

LIST OF ABBREVIATIONS

- AC- Law Reports, Appeal Cases (Decisions of the House of Lords and the Privy Council from 1891)
- ACLU- American Civil Liberties Union
- AG- Attorney-General
- Ala- Alabama
- All ER- All England Law Reports
- All NLR- All Nigeria Law Reports
- ALR- American Law Reports
- Am Jur- American Jurisprudence
- Am L Rev- American Law Review
- Am Rep- American Reports
- Ariz- Arizona
- Ark Stat Ann- Arkansas Statutes
- ATM- Automated Teller Machine
- BC- Borough Council
- BGB- *Bürgerliches Gesetzbuch* (German Civil Code)
- BGBI- *Bundesgesetzblatt* Federal Gazette Law
- BGH- *Bundesgerichtshof* (German Federal Court of justice- West Germany's Federal (Supreme) Court)
- BGHZ- *Entscheidungen des Bundesgerichtshofes in Zivilsachen* (Decisions of the West German Supreme Court in civil matters)
- BLR- Building Law Reports
- BVerfG- *Bundesverfassungsgericht* (Germany- Federal Constitutional Court)
- BVerfGE- *Entscheidungen des Bundesverfassungsgerichts* (Germany- Decisions of the Federal Constitutional Court)
- CA- Court of Appeal
- CA- Decision of the English Court of Appeal
- Cal- California

Calif Law Rev- California Law Review
 Cap- Chapter
 CC- Constitutional Court
 CC- County Council
 CCHCJ- Cyclostyled High Court Judgments (Selected Judgments of the High Court of Lagos State (Nigeria)
 CCTV- Closed Circuit Television Camera
 Ch- Law Reports, Chancery Division (from 1891)
 Circ- Circuit (Cases and decisions of the Federal Circuit Courts of Appeal- United States)
 CLR- Commonwealth Law Reports
 COE- Council of Europe
 Cr App R- Criminal Appeal Reports
 DLR- Dominion Law Reports (Canada)
 DPA- Data Protection Act
 DR- Decisions and Reports of the European Commission of Human Rights
 EC- European Community
 ECHR- European Court of Human Rights
 EGLR- Estates Gazette Law Reports
 EHRLR-European Human Rights Law Review
 EHRR- European Human Rights Reports
 EPIC- Electronic Privacy Information Center
 ER- The English Reports
 EU- European Union
 FSC- Federal Supreme Court (Selected judgments of the (abolished) Federal Supreme Courts of Nigeria- (1956-1961))
 F Supp- Federal Supplement (American law reports)
 F. 2d- Federal Reporter, 2nd Series (American law reports)
 FCC- Federal Constitutional Court
 FCR- Family Court Reporter
 FLR- Family Law Reports
 FRN- Federal Republic of Nigeria

FSR- Fleet Street Reports
 GLR- Ghana Law Reports
 Harv L Rev- Harvard Law Review
 HL- House of Lords
 ID- Identity
 ISP- Internet Service Provider
 KB- Law Reports, King's Bench (1901-52)
 LFN- Laws of the Federation of Nigeria
 LLR- Lagos Law Reports (Law Reports of the High Court of Lagos State, Nigeria)
 LRN- Law Reports of Nigeria
 LT- Law Times Reports (1859-1947)
 Media Law Rev- Media Law Review
 NCLR- Nigerian Constitutional Law Reports
 NJW- *Neue Juristische Wochenschrift* (Germany- New Law Journal))
 NLJ- New Law Journal
 NLR -Nigeria Law Reports
 NMLR- Nigerian Monthly Law Reports
 NWLR-Nigerian Weekly Law Reports
 NY- New York
 NYU Law Rev- New York University Law Review
 OECD- Organisation for economic Co-operation and Development
 PL- Public Law
 QB- Law Reports, Queen's Bench (1891- 1900; 1952-)
 QBD- Law Reports, Queen's Bench Division (1875- 1890)
 RGZ- *Entscheidungen des Reichsgerichts in Zivilsachen* (Germany-Decisions of the Imperial Court in Civil matters)
 RPC- Reports of Patent Cases
 SA- South Africa
 SACR- South African Constitutional Reports
 S Ct- Supreme Court
 S J- Solicitors' Journal

Syd Law Rev- Sydney Law Review

Tex- Texas

THRHR- *Tydskrif vir Hedendaagse Romeins-Hollandse Reg*

TLR- Times Law Reports

UILR- University of Ife Law Reports

UK- United Kingdom

US- United States of America

USC- United States Code (Laws made by the United States Congress)

VR-Victorian Reports (Australia)

WACA- West Africa Court of Appeal

WLR- Weekly Law Reports

SUMMARY

The right to privacy is one of the fundamental human rights affirmed in the Universal Declaration of Human Rights, in Article 12; in other international Covenants and Conventions; as well as in the Constitutions of many countries. Although some difficulty has attended the attempt to define privacy in legal terms, the right to privacy has generally been discussed in relation to such concepts as dignity, freedom to make choices for, or to be in control of information about, oneself, and the right to personality, amongst other related concepts.

Modern technology and the resultant increase in the rate of infringements of privacy have made the protection of privacy and data a pertinent contemporary issue. Prominent among the technology available today is the Internet. Ready access to, and ease of publication of information on the Internet are two of the major threats to privacy occasioned by the Internet. In response to the growing need for ready and affordable access to information as well as efficacious communication, which the Internet fulfills, Internet cafes have been set up in many developing countries. Further to the various threats to privacy occasioned by Internet use, the sharing of computers by members of the public in Internet cafes provides an operative medium for diverse acts of invasion of privacy and data.

In many countries of the world, South Africa and Nigeria inclusive, there are constitutional provisions as well as other statutes for the protection of privacy. In the

same vein, many countries have laws protecting data, and in some cases, there are comprehensive Data Protection Acts. In the United Kingdom, following a protracted reluctance by the Common Law courts to recognize a right to privacy, the incorporation of the Human Rights Act of 1998 into the domestic laws of the United Kingdom now guarantees the protection of privacy. However, there has been a Data Protection Act in operation in the United Kingdom preceding the recognition of the right to privacy.

In the United States, certain provisions of the Constitution have been construed to protect privacy rights, and the Common Law courts recognize a tort of privacy. Although there is no Data Protection Act in operation in the United States, there are several federal and state statutes protecting privacy and data. The German Constitution provides a foundation for the protection of privacy, and the German Civil courts have developed relevant Articles of the German Civil Code to provide protection for rights analogous to the right to privacy. Furthermore, the Germans have a system of Data Protection Acts, which are administered at both federal and state levels. Some of the above laws however have shortcomings that detract from their effectiveness.

In South Africa, the Roman and Roman-Dutch law which forms the foundation of South African Civil Law provides a basis for the protection of privacy through the protection of personality rights, and the South African courts have, for decades recognized and upheld rights analogous to privacy rights. As for data protection, although there are subject – specific statutes protecting data, there is no general South African Data Protection Act as yet. There is however a committee working on a draft Data Protection Act for South

Africa and it is expected that a comprehensive Data Protection Act will in time be enacted and operative.

In Nigeria, although the 1989 Constitution and previous Constitutions contain provisions guaranteeing the right to privacy, it is clear from the paucity of cases, that privacy and data protection are not an active area of law. As is the case in South Africa, there are subject specific Acts protecting data in Nigeria but no general Data Protection Act is in operation. A challenge thus exists to develop and utilise the constitutional guarantee of the right to privacy as well as available tort law for effective privacy protection in Nigeria. The need for appropriate data protection legislation in Nigeria is also evident.

In this work, the privacy and data protection laws in South Africa and Nigeria are examined, with particular reference to the processing of information in Internet cafes. Of concern, during the final stages of the drafting of this work was the submission of a similar thesis in another university.¹ However, in spite of a general similarity in topic, and common sources of authority, there are major points of departure in each work. While this research is a comparative study of the privacy and data laws in Nigeria and the South Africa with specific focus on Internet cafes, the other work does not examine the law in Nigeria, nor does it focus on Internet cafes.

¹ A Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* University of South Africa (October 2003).

The examination of German privacy and data laws for comparative purposes in this work, as opposed to the use in the other work, of the privacy and data laws in the Netherlands, is another major difference in the two theses. Yet another point of departure is the discussion in the other work, of certain data technology such as credit cards and information held by credit bureau, which are not as commonly used in Nigeria as in South Africa. As such, they do not provide a suitably balanced basis for comparison between Nigeria and South Africa for the purpose of this research, and therefore, have not been focused on.

Following examination of the South African and Nigerian privacy and data protection laws, general principles to be included in a privacy law and Data Protection Act for the protection of privacy and data in Internet cafes will be proposed for Nigeria. In the present dispensation of technological advancement, until the law can provide adequate protection for privacy and data by the prevention of infringement as opposed to the prescribing of retribution to offenders, or the provision of compensation to victims, the protection of privacy and data will continue to be a pertinent issue.

CHAPTER ONE

INTRODUCTION: THE CHALLENGE OF INFORMATION TECHNOLOGY TO PRIVACY

1.1 The Right to Privacy

The word “privacy” and the concept of privacy are common in everyday speech and usage. Privacy has been variously defined¹ and in law, the concept of privacy has been described as “an amorphous and elusive one”.² For the purpose of clarity, it is important to attempt a definition of the scope of privacy in law. It is also necessary to delimit the scope of the right to privacy because like every legal right, the right to privacy is not absolute or without limit.³

The right to privacy is essentially, the right of an individual to keep certain aspects of his or her life and, or person to himself/ herself and to be free from interference in respect of

¹ R. Wacks *The Protection of Privacy* (1980) at 10 & 11. Privacy has been described as a “right”, “condition”, “state”, “area of life” and is also widely defined in terms of “control”.

² Ackermann J in *Bernstein v Bester* NO 1996 (2) SA 751 (CC) at Para 65.

³ For instance, in spite of the importance of the fundamental rights entrenched in Chapter IV of the Constitution of Nigeria (1999), and the rights in Chapter 2 of the South African Constitution, (1996); both Constitutions contain provisions limiting these rights in Section 45 of the Nigerian Constitution and Section 36 of the South African Constitution respectively: See also Ackerman J in *Bernstein v Bester* op cit: “[F]rom the outset of interpretation each right is always already limited by every other right accruing to every other citizen.”

this secluded area.⁴ The issue of privacy has long been a legal concern and there is an abundance of jurisprudence on the right to privacy.⁵ Some of the available definitions and theory will be briefly examined in the following paragraphs.

It has been said that the right to privacy is used to refer to a sphere of personal autonomy, which is protected by the law from interference.⁶ It has also been asserted that at the very least, the right to privacy includes the right to be free from intrusions and interference by the state and others in one's personal life.⁷ In this regard, searches, interception of correspondence, wire or telephone tapping, the use of electronic surveillance or other bugging devices, recording, photographing or filming, amongst others, have been identified as aspects covered by the right to privacy.⁸

In delimiting its scope, the right to privacy has been recognised in relation to such legal concepts as autonomy, property, dignity, reputation, confidentiality, and secrecy, among others.⁹ Although the scope of privacy has also been described as closely related to the

⁴ See generally J Neethling, J M Potgieter, P J Visser *Law of Delict* (2006) 5th ed at 335, See also D McQuoid-Mason "Privacy" in M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz, S Woolman (eds) *Constitutional Law of South Africa* (2004) at 38-1. Cf also Anneliese Roos *The Law of Privacy (Data) Protection: A Comparative and Theoretical Study* (2003) at 555.

⁵ W P Keeton, D B Dobbs, R E Keeton & D G Owen *Prosser and Keeton on the Law of Torts* (1984) at 850. Cf Roos op cit at 29.

⁶ I J Sloan *Law of Privacy Rights in a Technological Society* (1986) at 13; Cf Corbett J A in *S v Naude* (1975) (1) SA 681 (A) at 704A-B, where he describes the right of the individual to privacy thus: "such privacy as the law allows him" See also Ackermann J in *Bernstein v Bester* op cit at Para 75 where he observes that the law will only protect a claim to privacy where it recognises that there is a "legitimate expectation of privacy".

⁷ McQuoid-Mason in Chaskalson et al op cit at 38-1.

⁸ Ibid.

concept of identity,¹⁰ there is authority to support the view that identity is an independent personality right (in Civil Law jurisdictions).¹¹

Following the publication of Warren and Brandeis's Law Review Article in 1890,¹² the right to privacy became commonly described as "the right to be let alone to live one's own life with the minimum degree of interference."¹³ This definition of privacy has been said to include the following aspects:

"the right of the individual to lead his own life protected against interference with his private, family and home life; interference with his physical or mental integrity or his moral and intellectual freedom; attacks on his honour and reputation; being placed in a false light; the disclosure of irrelevant embarrassing facts relating to his private life; the use of his name, identity or likeness; spying, prying, watching and besetting; interference with his correspondence; misuse of his private communications, written or oral; disclosure of information given or received by him in circumstances of professional confidence".¹⁴

⁹ See generally Wacks op cit at 12ff.

¹⁰ Rainer Forst "How not to Speak About Identity: The Concept of the Person in a Theory of Justice" in *Philosophy and Social Criticism* (1992) Vol 8 No 1.

¹¹ See *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* (1977) 4 SA 376 (T) 386, Cf (1979) 1 SA 441 (A) 456, where the right to identity was recognised as an independent right of personality. See also *Grütter v Lombard* 2007 (4) SA 89 (SCA), (3) All SA 311 (SCA) Cf Neethling et al op cit at 356.

¹² "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

¹³ Cf The declaration of the Nordic Conference of Jurists on the Right to Respect for Privacy Paras 2 & 3.

¹⁴ Ibid.

Prosser, in his celebrated Article¹⁵ identified the following four categories of interests protected by the right to privacy: intrusions, public disclosure of private facts, publicity which places the plaintiff in a false light, and appropriation of plaintiff's name or likeness for the benefit or advantage of another.

The right to privacy has been used in a "narrower sense in the aspect of personal autonomy, to refer to the power of choice and control".¹⁶ It has been said that:

"The essence of privacy is ...the freedom of the individual, to pick and choose for himself [or herself] the time and circumstances under which, and most importantly, extent to which, his attitudes, beliefs, behaviour and opinions are to be shared with or withheld from others. The right to privacy is, therefore, a positive claim to a status of personal dignity..."¹⁷

¹⁵ W L Prosser "Privacy" (1960) 48 *California Law Review* 383.

¹⁶ Sloan op cit at 13. Cf also Roos op cit at 556 where she observes that the right to determine the scope of one's interest in privacy is the essence of the individual's interest in his or her privacy.

¹⁷ O M Ruebhausen & O G Brim "Privacy and Behavioural Research" (1965) 65 *Columbia Law Report* at 1185. Cf C Fried "Privacy" (1968) 77 *Yale Law Journal* 483: "Privacy is not merely an absence of information about an individual in the minds of others, but rather the individual's *control* over the information he has about himself". See also A F Westin *Privacy and Freedom* (1967) 33ff:

"The most serious threat to the individual's autonomy is the possibility that someone may penetrate the inner zone and learn his ultimate secrets ... This ...would leave him naked to ridicule and shame and would put him under the *control* of those who knew his secrets."

See also *Griswold v Connecticut* (1965) US 479 at 484 on 'zones of privacy'; *Bernstein v Bester* supra at 788ff on "a multi-levelled recognition of identity". Here, Ackermann J states that only the "inner sanctum" of a person is protected from interference, and that the "scope of (a person's) personal space shrinks" as one moves into communal relations and activities.

Clearly, not all information, or aspects of one's life fall within the secluded area protected by the law of privacy; the scope of a person's right to privacy will be limited to personal information about him or her.¹⁸

Bloustein in his article,¹⁹ written as a rejoinder to Prosser's article classifying the interests protected by the law of privacy into four, wrote that there is only one interest protected by the law of privacy, which is "human dignity." The view that the right to privacy protects a person's dignity has long existed. Roman law recognition and protection of the dignity (and reputation) of the person dates back to 450 BC.²⁰ Although Roman law does not specifically mention the right to privacy, it does provide for the protection of many of the rights that have come to be recognised under the law of privacy.²¹ In South Africa and other civil law countries the right to privacy is based on the Roman concept of *dignitas* or "dignity in the broad sense".²²

There is a distinction between the Common Law and Civil Law protection of the right of privacy. The root of the action in Common Law systems is a mixture of property law and dignity.²³ With regard to property, it is noteworthy that in the 16th century, Locke in his

¹⁸ Cf Roos op cit at 556.

¹⁹ E J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 *NYU Law Review* 962, 964.

²⁰ D J McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 13.

²¹ Ibid.

²² See Ackermann J in *Bernstein v Bester* supra at 789.

²³ See below Chapter 4.

theory of private property was of the opinion that; “everyman has a ‘property’ in his own ‘person’; this, nobody has a right to but himself”.²⁴ John Stuart Mill, affirming this position in later years, states: “Over himself, over his own body and mind, the individual is sovereign.”²⁵

In this light, it is noteworthy that, even though there is no Common Law right to privacy in the United Kingdom, English Common Law offers protection in respect of certain rights that are analogous to privacy rights, based on the principle of protection of property rights.²⁶ In Civil Law systems however, the root of the action does not lie in property rights,²⁷ it is recognised as an independent personality right.²⁸

As observed earlier, no right is absolute in law since each legal right asserted by one is often a limitation of the right of another.²⁹ While the individual’s right to privacy, honour and reputation should be affirmed and protected, the exercise of the freedom to see, hear, speak, and learn must also be protected and should only be curtailed for a good cause.³⁰ Moreover, the free flow of information enhances public enlightenment and education,

²⁴ J Locke *The Second Treatise of Civil Government* (1986) at 129.

²⁵ J S Mill *Utilitarianism Liberty Representative Government* (1962) at 73.

²⁶ See *Albert v Strange* [1849] 2 De G & Sm 652, 64 ER 293 (Ch), *Herbert Morris Ltd v Saxelby* [1916] 1 A.C. 688 at 714, *Rolls Royce Ltd v Jeffrey* [1962] 1 All ER 801 at 805.

²⁷ Ibid. See also Ackermann J in *Bernstein v Bester* supra at Para 68.

²⁸ Neethling et al op cit at 18.

²⁹ See above at 1.

³⁰ See generally J Burchell *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum* (1998) at 12ff. See also Sloan op cit at xvi.

which are essential for progress and development in every society. The law must strike a just balance between these conflicting interests.³¹

Under the English Common Law, when weighing the right to be free from interference from others³² or the right to prevent others from disclosing facts or information about one's private life,³³ against other interests, the consequences have often been considered. The question here is whether there is damage or injury to something, which could be treated as property, such as the commercial value of a name, or picture, or business information.³⁴ In such cases, limited protection may be found in the law of tort.³⁵

The law also considers whether the information was revealed under circumstances where a duty of confidence existed or could be imposed.³⁶ Where there is such a duty, the courts are more inclined to affirm a right of privacy.

³¹ Ibid. See Cameron J in *Holomisa v Argus Newspapers Ltd* (1996) (2) SA 588 (W) at 608-9.

³² The Common Law courts did not recognise a right to privacy until the Human Rights Act (Chapter 42 of 1998) came into force. See *Kaye v Robertson* [1991] FSR 62; Lord Nolan in *R v Khan* [1997] AC 558 at 581. See below Chapter 3.

³³ This was usually based on the principle of confidentiality. See *Argyll v Argyll* [1965] 1 All ER 611, 620 (HOL), (1967) Ch 308.

³⁴ *Herbert Morris Ltd v Saxelby* [1916] 1 AC 688 at 714, *Technograph Printed Circuits Ltd v Chahoyan* [1967] RPC 399 at 344.

³⁵ For instance, in *Rolls Royce Ltd v Jeffrey* supra “know-how” was described as a corporate “asset” distinct from the physical records in which it was contained. (Per Lord Radcliffe at 801). Also, the tort of passing off protects commercial interests. It provides relief against unfair use of a business “get-up” or trade name.

³⁶ *Argyll v Argyll* supra, *Morison v Moat* [1851] 9 Hare 241.

With the coming into force of the Human Rights Act,³⁷ which incorporates part of the European Convention on Human Rights including Article 8, which provides for the right to privacy, the courts are no longer limited to the above criteria to protect privacy rights.³⁸ In effect, the plaintiff in a case of invasion of privacy does not have to prove damage to property, injury to his person, nuisance or breach of confidentiality in order for the courts to affirm a right to privacy, since the Convention expressly guarantees this right.

In Civil Law systems, the Common Law action was based on infringement of personality rights, and not property rights.³⁹ The courts in South Africa have recognised the right to privacy as an independent personality right that falls under the concept of *dignitas*.⁴⁰ The courts have also identified three essential components that must be proved in order to establish liability for injury to personality.⁴¹

At Common Law the requirement for recognition of the existence of a duty to protect in cases where a person's private affairs were interfered with would generally be unlawful

³⁷ Chapter 42 of 1998; The Act came into effect in England on 1 October 2001, and in Scotland on 1 October 2000.

³⁸ Section 6; See below Chapter 3.

³⁹ *Bernstein v Bester* supra.

⁴⁰ Neethling et al op cit at 354. See also *Financial Mail (Pty) Ltd v Sage Holdings Ltd* (1993) 2 SA 451(A) 462-463; *Nell v Nell* (1990) 3 SA 889 (T), *O'Keefe v Argus Printing and Publishing Co Ltd* (1954) 3 SA 244 (C).

⁴¹ *R v Umfaam* (1908) TS 62 66, per Innes CJ; See also *Boswell v Union Club of SA (Durban)* (1985) 2 SA 162 (D) 164-165, *SAUK v O'Malley* (1977) 3 SA 394 (A) 402. See below Chapter 4.

or unreasonable interference with property⁴² or the establishment of a duty of confidentiality, a Civil Law analysis of the requirements of the right to privacy would be: (a) unlawfulness (b) fault, and (c) infringement of a personality right.⁴³

Under Common Law, there are, however certain torts that may afford protection for the right to privacy, in respect of which emotional distress⁴⁴ and intention to cause physical harm⁴⁵ or damage to reputation,⁴⁶ and not interference with property, must be proved.

1.2 Data Protection

Data may be regarded loosely as recorded or, processed information.⁴⁷ The focus in this work will primarily be on personal data. However, business information including information relating to juristic persons will also be discussed. Westin, writing about four decades ago, identified physical surveillance, psychological surveillance and data surveillance⁴⁸ as three major areas in which the technological revolution in surveillance

⁴² *Anchor Brewhouse Developments v Berkley House (Docklands Developments)* [1987] Ch D 2, *Khorasandjian v Bush* [1993] QB 727.

⁴³ See *McQuoid-Mason* op cit at 100 ff; See below Chapter 4.

⁴⁴ *Janvier v Sweeny* [1919] 2 KB 316.

⁴⁵ *Wilkinson v Downton* [1897] 2 QB 57.

⁴⁶ *Tolley v J S Fry and Sons Ltd* [1931] AC 333.

⁴⁷ Cf Section 1(1) of the United Kingdom Data Protection Act Cap 29 of 1998. See Para 3.2.2.2.2 below for full of definition of data as contained in the United Kingdom Data Protection Act 1998.

⁴⁸ Westin op cit at 68; Cf the definition of privacy in a resolution of the Consultative Assembly of the Council of Europe adopted by Ackermann J in *Bernstein v Bester* supra at 791: “ The right to privacy concerns ... physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs ... ”

techniques posed a threat to privacy. The maintaining of records containing personal information has been in practice for centuries.⁴⁹ With the proliferation of data banks and computerised pools of information, where vast amounts of information or data are stored, there is greater possibility of invasion of privacy through the misuse of information or personal data.⁵⁰

Although data is not deliberately or routinely collected in Internet cafes, customers often process personal information in Internet cafes. Processing has been so broadly as to accommodate most, if not all operations performed upon personal data.⁵¹ This includes, but is not limited to the collection, storage, recording, collation or sorting, updating, modification, alignment, combination, sharing, linking, deletion or destruction of data.⁵²

Curriculum vitae and information contained in e-mail exchanges between family members, friends or businesses when retained in a computers' hard drive, qualify generally as data⁵³ and are commonly processed in Internet cafes. In addition to this, when visited, many websites have devices that collect and record information relating to

⁴⁹ Cf Roos op cit at 1 ff.

⁵⁰ Cf J Neethling *Neethling's Law of Personality* (2005) 2nd ed at 295, where he states that the processing of information by the data media constitutes a threat to the individual's privacy and may also lead to an infringement of his (or her) identity. See also McQuoid-Mason op cit at 295-6.

⁵¹ Cf Roos op cit at 552.

⁵² Cf Section 1(1) of the United Kingdom Data Protection Act Cap 29 of 1998.

⁵³ Cf also Roos op cit at 557 where she observes that separate pieces of information about a person which are not necessarily private, may, when put together create a picture or record that the individual would like to restrict others from having knowledge of.

the customer.⁵⁴ Such information may also qualify as data and is open to misuse by a malefactor.

The compilation and distribution of personal information,⁵⁵ and the acquisition and disclosure of false or misleading data have been identified as ways in which the processing of information by data media poses a threat to personality.⁵⁶ Apart from the obvious risk of data being accessed or disclosed unlawfully, data processed may also be irrelevant, incomplete or inaccurate, or, used for a purpose other than that for which they were collected.⁵⁷ In the present day, data is processed in a variety of ways that pose an even greater threat to privacy. Some of these different forms of processing include data matching, profiling, data mining, cookies⁵⁸ and spam.⁵⁹

Data matching involves the use of a common denominator (for instance identity number) to compare records held by different agencies regarding persons included in more than one file.⁶⁰ Data mining involves the analysis or “mining” of existing databases to reveal

⁵⁴ Cf above Para 1.2.

⁵⁵ These, according to Neethling, create a direct threat to the individual’s privacy. See Neethling op cit at 295.

⁵⁶ Neethling op cit at 295 considers these threats to identity. Cf Roos op cit at 554, who asserts that the processing of true personal information leads to an infringement of privacy, while identity is infringed where false or misleading information is processed.

⁵⁷ Cf Roos op cit at 6 & 7.

⁵⁸ Cf above at 12.

⁵⁹ See generally Roos op cit at 8-12. Many of these forms of processing are not common in Nigeria therefore they are not discussed in great detail here.

⁶⁰ Cf Roos at 8.

previously hidden information using new search techniques.⁶¹ Profiling involves the search of record systems for a specific set of historical factors for the purpose of making a judgement about a particular individual on the basis of the past behaviour of other individuals who share similarities in physical, socioeconomic, cultural or demographic characteristics.⁶²

Data protection laws regulate the collection, disclosure and use of information stored in data banks. Data protection entails the legal protection of a person (the data subject) with regard to the processing of data concerning him or her by another person or institution (the data medium).⁶³ It has been pointed out that, for data protection law to be effective, a data subject must be “legally empowered to exercise direct *control*”⁶⁴ over his data records.”⁶⁵ In this regard, Neethling⁶⁶ highlights certain requirements necessary to facilitate individual control over personal records.⁶⁷ According to him,

⁶¹ Cf Roos op cit at 10.

⁶² Cf Roos at 8-10.

⁶³ Cf Neethling op cit at 291.

⁶⁴ Cf above Para 1.1. where privacy is defined in terms of the individual’s “control” over information about him/herself. See also McQuoid-Mason in Chaskalson et al at 38.1.

⁶⁵ Neethling op cit at 303ff. See also Burchell op cit at 398.

⁶⁶ Neethling op cit at 303.

⁶⁷ Cf Articles 10 – 12 of the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data. (Directive 95/46/EC 1995). See also R Buys (ed) *Cyberlaw @ SA II: The Law of the Internet in South Africa* (2004) 2nd ed at 379-380.

“The individual must (i) be aware of the existence of the data record concerning him or her stored at a particular data medium⁶⁸ (ii) be aware of the purpose(s) for which data is processed⁶⁹ (iii) be legally entitled to have access to his or her data records⁷⁰ (iv) be legally entitled to acquire information as to which person have or have had access to his or her data records;⁷¹ and (v) be legally empowered to procure a correction or deletion of certain data.”⁷²

As will be shown,⁷³ another essential factor affecting the effectiveness of any data protection law is the mode of enforcement of that law. In enforcing different data Protection Acts, there are different models of data protection adopted by different countries. Systems that provide for a public official who enforces a comprehensive data protection law, such as exist in the United Kingdom and Germany have been described as having a regulatory model of data protection.⁷⁴

⁶⁸ Cf Section 7 (1) (a) of the 1998 the United Kingdom Data Protection Act.

⁶⁹ Cf Section 7 (1) (b) United Kingdom Data Protection Act.

⁷⁰ Cf Section 7 United Kingdom Data Protection Act.

⁷¹ Cf Section 7 (1) (b) United Kingdom Data Protection Act.

⁷² Cf Section 14 United Kingdom Data Protection Act.

⁷³ Below Paras 3.2.2.2.2 and 3.3.3.1.1.

⁷⁴ See D Banisar & S Davies “Privacy and Human Rights: An International Survey of Privacy Laws and Practice” at <http://www.gilc.org/privacy/survey/intro.html#defining>. This is also the system adopted in Australia: the (Commonwealth) Privacy Act [1988 as amended by the Privacy Amendment Act 1990 & the Privacy Amendment (Private Sector) Act 2000]; Canada: the Privacy Act (1980-83 c 111, Sch. 11 “1”) and the Personal Information Protection and Electronic Documents Act (2000, c.5); New Zealand: the New Zealand Ombudsman Act (1975) and many European countries.

The job of the official includes monitoring compliance with the law and conducting investigations into alleged breaches.⁷⁵ The official is also responsible for public education and international liaison in data protection and data transfer.⁷⁶

The title given to the official varies from country to country, such as “commissioner”,⁷⁷ “registrar”,⁷⁸ or “ombudsman”,⁷⁹ as do the powers.⁸⁰ In Germany, in addition to adopting the regulatory model, there is a Federal Data Protection Act⁸¹ and each state also has its own data protection law.⁸² The model of data protection adopted in a country affects the overall usefulness of the law. A good data protection Act or law will only be effective to

⁷⁵ See generally Parts III, V & VI of the United Kingdom Data Protection Act (Cap 29 of 1998). See also Section 37 of the Canadian Privacy Act (1980) and Sections 34-36 of the Canadian Access to Information Act (1982).

⁷⁶ See Schedule 5 of the United Kingdom Data Protection Act.

⁷⁷ E.g. the United Kingdom (Section 6 Data Protection Act 1998), and Canada where there are two separate commissioners- an information Commissioner and a Privacy Commissioner- whose offices are provided for by two different, but complementary Acts. See the (Canadian) Privacy Act 1980 (section 37) and the (Canadian) Access to Information Act 1982. (See Sections 30-39).

⁷⁸ In the United Kingdom, section 3 (1) (a) of the repealed 1984 Data Protection Act (Cap 35) provided for a Data Protection Registrar whose duties were administrative and supervisory.

⁷⁹ E.g. New Zealand; See generally the (New Zealand) Ombudsman Act (1975). See also N Marsh (ed) *Public Access to Government-Held Information* (1987) at 226ff. It is noteworthy that by virtue of Section 36(2) of the 1984 United Kingdom Data Protection Act, the Data Protection Registrar is also empowered to perform the duty of ombudsman. Cf P Birkinshaw *Government & Information; The Law Relating to Access, Disclosure & Regulation* (1990) pp 208-9.

⁸⁰ It appears that in spite of the differences in title, the basic duty of each official is to monitor compliance with the various Data or Information Acts, to perform administrative and supervisory duties, and to generally function as an ombudsman. In this regard, the powers of the officials, by whatever name called, are very similar. Cf Marsh op cit at 159, where he observes that the office of the Information Commissioner in Canada is modelled on that of an ombudsman.

⁸¹ *Bundesdatenschutzgesetz*; Federal Data Protection Act of 27 January 1977.

⁸² Cf below Para 3.4.3.2.

the extent that the provisions are enforceable, and that the law provides for a suitable administrative and legal framework for this.⁸³

Data protection can fill the lacuna in the protection of personal information where the protection afforded by the law of privacy is inadequate or is not sufficiently detailed.⁸⁴

For our purpose, the issue of data protection is relevant when discussing the protection of privacy in Internet cafes because cases involving encroachment on electronic mail or personal information retained on a computer ultimately involve the wrongful use of personal information or, the infringement of data.

There will be an overlap between the interests protected by privacy and the data protection laws.⁸⁵ It has been said that privacy protection may include freedom from unauthorised disclosure about one's personal life.⁸⁶ More specifically, data and privacy protection will overlap where the misuse of data falls into one of the categories specified by Prosser⁸⁷ viz: intrusions, publication of private facts, appropriation of a person's name or likeness for the benefit of another or false light.

⁸³ Cf below the United States of America Privacy Act of 1974 at Para 3.3.3.1.1.

⁸⁴ For instance, in England, until the coming into effect of the Human Rights Act (Cap 42 of 1998), the Common law did not recognise a right to privacy. See below Chapter 3.

⁸⁵ C Reed *Internet Law: Text and Materials* (2004) 2nd ed at 227 identified a good privacy law to consist of "a definition of the circumstances in which third parties have the right to collect, use and disseminate personal information about others; and a mechanism for preventing collection, use and dissemination outside those limits".

⁸⁶ McQuoid-Mason in Chaskalson et al op cit at 38-1.

⁸⁷ Cf above at 1.

For instance, where personal information contained in a data bank is unlawfully accessed by a data controller,⁸⁸ and such data is subsequently unlawfully published or otherwise misused,⁸⁹ action will lie for data infringement under the relevant Data Protection Act for unlawful use and disclosure of information and it will also be possible to bring action for invasion of privacy in respect of the unlawful intrusion and publication and. Thus, for instance, where an Internet café owner or worker obtains personal information stored on a computer without lawful authorization and publishes or otherwise discloses the information, action will lie for invasion of privacy as well as for data infringement.

It must be pointed out here that although in the discussion of their protection, privacy and data protection are sometimes used interchangeably,⁹⁰ a subtle distinction exists between the two. While data protection relates to information processed manually (in writing) or automatically,⁹¹ privacy protection covers infringements upon personal information as well as personal space and dignity.⁹² For instance, while it may qualify as invasion of privacy to secretly watch a person undress⁹³ or bath,⁹⁴ or to take photographs,⁹⁵ these acts do not ordinarily constitute a violation of any data protection law. Moreover, while

⁸⁸ Cf below for the definition of data controller.

⁸⁹ See generally Baer op cit at 134-5; See also Sloan op cit at 6ff.

⁹⁰ See generally Roos op cit at cover page ff.

⁹¹ Part I Section I United Kingdom Data Protection Act 1998.

⁹² Cf above Para 1.1. See *R v Jungman* 1914 TPD 8 at 10,11 Cf at Para 3.2.2.1.2.2.

⁹³ *R v Holliday* 1927 CPD 395 at 401; *R v Daniels* 1938 TPD 312 at 313.

⁹⁴ *R v Schoonberg* 1926 OPD 247.

⁹⁵ See *Douglas v Hello! Ltd* [2001] QB 967, [2002] 1 FCR 289, [2003] EWHC 786.

data protection laws are often designed to be enforced against data agencies and not private individuals, the right to privacy may be enforced against private and corporate individuals and government agencies alike. It is submitted that although data and privacy protection rights overlap, the scope of privacy protection is wider than data protection. In line with this position, data and privacy are discussed separately in this paper but any reference to privacy does not exclude data unless expressly stated herein.

1.3 Modern Day Invasion of Privacy

With the development of technology, there has been a corresponding enhancement of the ability to obtain information. This is evidenced by the constant upgrade of, and improvement on audio and video equipment as well as other devices for obtaining information. For instance, microphones and hearing pieces that can record far and distant sounds, even as low as whispers, are readily available, and the art of telephone tapping, though not new,⁹⁶ has been significantly improved upon..⁹⁷ Today, laptop and palmtop computers, flash drives and other minute computer accessories that are easy to transport and which facilitate virtually unlimited access to, mass storage and easy transfer of information are commonly used.

⁹⁶ Many of the technological developments mentioned are not new. Cf Justice Brennan in *Lopez v United States* (1963) 373 U S 479 where he observed that:

“Electronic eavesdropping by means of concealed microphones and recording devices of various kinds ... permit a degree of invasion of privacy that can only be described as frightening”.

However, modifications are constantly being made to increase the efficiency of these devices, thus greatly facilitating invasions of privacy.

⁹⁷ Through modern technology, physical presence has become less important for planting bugs. See S Garfinkel *Database Nation The Death of Privacy in the 21st Century* (2000) at 108ff.

Although the use of photography as a means of identification for the purposes of crime control is “nearly as old as the camera itself”⁹⁸, it is clear that photography today is radically different from what it was two centuries ago. Today electronic eavesdropping and electronic surveillance⁹⁹ through advanced photography¹⁰⁰ is affordable and often engaged in, in some form by many families.¹⁰¹

Many effective ways of surreptitiously listening to, watching and tagging the individual abound and are being created in the present day.¹⁰² In the common place and regular activities of life, such as grocery shopping,¹⁰³ collecting ‘quick’ cash from the automated teller machine,¹⁰⁴ using a credit card to make payment, walking into an office or shop where entry is allowed using a magnetic stripe pass,¹⁰⁵ one is constantly being

⁹⁸ Norris & Armstrong op cit at 13-18.

⁹⁹ There is a proliferation of home surveillance systems and it is possible to record video tapes through a portable camera and wireless receiving screen, or pre-set the device to record without physical presence. See Garfinkel op cit at 108.

¹⁰⁰ Digital video cameras are portable devices with which one can make video recordings through one’s personal computer, pictures taken can also be sent easily via e-mail, thus facilitating intrusions as well as publication of information. See Garfinkel op cit at 108.

¹⁰¹ For instance as a security measure, there are homes with cameras attached to the doorbell system and in some cases, cameras are installed within the homes. Cf fn 46 above.

¹⁰² See generally Lipschultz op cit at 225ff; See also C Norris & G Armstrong *The Maximum Surveillance Society* (1999) at 210-219.

¹⁰³ In the United States of America, grocery stores allow customers to register for discount coupons that are used to track what they purchase. See H Henderson *Privacy in the Information Age* (1999) at 23. See also J Quittner “Invasion of Privacy” *Time* (August 25 1997) at 38.

¹⁰⁴ The bank records time, date and location of the transaction as reflected on the receipt slip.

¹⁰⁵ Whenever a magnetic stripe pass is relied upon to enter any premises, one’s whereabouts are automatically recorded. See Quittner op cit at 38.

photographed and personal transactions are recorded.¹⁰⁶ Virtually every business transaction done today is with the use of computer facilities, and the constant surveillance made possible by these technological devices in everyday transactions is an incursion into one's freedom and on the right to privacy.

In the same light, cellular phones have become commonly used in all walks of life - by college and varsity students, different classes of workers ranging from business executives to cleaners, and even school pupils. Apart from providing the ability to communicate while in transit, messages can be sent and received on cellular phones at very little cost via the Short Message System (SMS).

Cellular phone technology also makes the transfer and downloading of information through the Internet possible. However, calls made on cellular phones can easily be intercepted and accessed and numbers can be identified with scanners by eavesdroppers.¹⁰⁷

Modern day technology also makes it possible to watch consumers without their consent and to determine their tastes and preference.¹⁰⁸ For instance, there are software programs that "commandeer" a person's computer to spy on him or her.¹⁰⁹ Furthermore, while

¹⁰⁶ Norris & Armstrong op cit at 3.

¹⁰⁷ See Henderson op cit at 23, see also Quittner op cit at 38.

¹⁰⁸ J H Lipschultz *Free Expression in the Age of the Internet- Social and Legal Boundaries* (2000) at 225-228. See also Henderson op cit at 22-23.

browsing on the web, many sites tag visitors with “magic cookies”¹¹⁰ that record what they are looking at and how long they have been “surfing”.¹¹¹ These are only some of the many ways in which technology has come to affect everyday life and threaten the right to privacy.

Further to this, present day technology makes it necessary to give and have stored in a database such information as names, addresses, and telephone numbers, at the very least, for many ordinary transactions performed daily. Particularly, in the use of the Internet, one often has to give personal information including one’s name, address, date of birth, and, sometimes, banking details in order to access or receive needed services or information.¹¹²

Apart from the threat to privacy posed by the necessity to give personal information, the internet also provides an easy means of publishing any information to specific persons, using their e-mail addresses. Every electronic-mail message has a header which contains some information about the sender and recipient(s) of the message.¹¹³ Furthermore, community based e-mail makes it possible to provide advertisers with the name, telephone number, address, e-mail and other personal details of almost every Internet user

¹⁰⁹ The software plants itself in the depths of the hard drive, “digs up” information from there, and sends the information gathered back “home”. A Cohen “Spies Among Us” in (*Time* July 31 2000) at 38.

¹¹⁰ Cookies are bits of data that can be stored on one’s personal computer. They are also used to keep a record of visitors to websites. See also Cohen op cit at 38.

¹¹¹ Cohen op cit at 38.

¹¹² Cf Buys op cit at 365.

¹¹³ Ibid.

who sees them.¹¹⁴

On a larger scale, the Internet is like a universal notice board that anyone can easily access with a computer. It has been described as both a “shopping mall” or “library”¹¹⁵ and “common-carrier” medium, where “individuals have the power to be their own publishers.”¹¹⁶ The ease with which one can access the Internet both for the purposes of obtaining and publishing information poses a significant threat not only to the privacy of individuals, but also of organisations and governments. Any skilled computer user can anonymously publish any information on the world’s most public bulletin board- the Internet.¹¹⁷ The Internet has been described as an “abattoir” for secrets.¹¹⁸

In spite of these threats to privacy, the utility of the internet in providing information and as a means of communication is unmatched, therefore internet communication is performed and business transactions are conducted via the internet, daily across the world. In order to meet present day demands for affordable communication, and access to

¹¹⁴ “South Africa Urged to Take the Lead in Updating Privacy Laws for Internet” (1999) <http://www.itweb.co.za/sections/techforum/1999/991106810115.asp> Accessed September 2000. See generally Henderson op cit at 23 ff. See also *Avrahami v US News & World Report* (1996) CCA, Virginia NO 95-1318.

¹¹⁵ In *Reno v American Civil Liberties Union* (1997) 117 SCt 2329, the Supreme Court rejected the argument that the World Wide Web could be viewed as a broadcast medium, instead, they found it analogous to a library or a shopping mall.

¹¹⁶ Lipschultz op cit at 10.

¹¹⁷ In *Zeran v America Online* 129 F. 3d 327 (4th Cir. 1997) where defamatory messages were posted on the defendants website by an unidentified third party, the court held that the plaintiffs were not responsible for liability that originates with third parties.

¹¹⁸ A Farham “How Safe Are Your Secrets?” in *Fortune* September 8, 1997.

information via the internet in some countries, South Africa and Nigeria inclusive, Internet cafes have been created.

1.4 Internet Cafes

In order to establish certain issues concerning the use of Internet cafes, a field study was conducted in South Africa and in Nigeria. To this end, interviews and questionnaires were administered to Internet café users in Nigeria and in South Africa.

Some of the general issues sought to be determined include the mode of operation of Internet cafes, the level of usage of Internet cafes by the public in South Africa and Nigeria, as well as issues surrounding the perceptions and opinions of Internet café users on privacy and the Internet. Findings from the field study have been incorporated in this work. More information about the field study can be found in the appendix.¹¹⁹

An Internet café is a business set-up situated in a room or enclosure, where computers providing Internet access are made available for public use at a fee.¹²⁰ There are two basic services provided in such Internet cafes: the sending and receiving of personal e-mail and access to information on the World Wide Web.¹²¹ In research conducted in

¹¹⁹ Below at 467

¹²⁰ Definition formulated based on the writer's observation of the set-up of, and the practice in, several Internet cafes in Nigeria and South Africa, and from interviews with different Internet café owners and users. Internet cafes usually charge customers a fixed rate for every minute spent on the Internet. Cf Appendix at Para 1.1

¹²¹ Ibid.

South Africa and in Nigeria 2003¹²² it was established that as of 2003, Internet cafes were commonly used in both countries.

Internet cafes represent a threat to privacy in the following ways. Firstly, the fact that there are several users of the same number of computers creates a situation where information intended for one user may be accessed by others, either inadvertently or deliberately. A skilled computer user could hack into any of the computers in an Internet café and retrieve information with relative ease. However, even where there is no intent to do wrong, it is possible for a computer user to access information intended for a previous user where the previous user did not log out properly.

In this regard, 46% of the Internet café users questioned in Nigeria were aware of the potential for invasion of privacy,¹²³ and all them,¹²⁴ as well as all the Internet cafes owners interviewed,¹²⁵ identified “incorrect logouts” as one of the commonest ways by which others might access personal information intended for other users.

In South Africa, only 22% of Internet café users questioned thought that the use of Internet cafes posed a threat to their privacy.¹²⁶ However, 90% of the Internet café owners interviewed in South Africa were of the opinion that the use of Internet cafes held

¹²² See generally below Appendix.

¹²³ Cf below Appendix at Para 1.6.1b.

¹²⁴ Ibid.

¹²⁵ Cf below Appendix at Para 1.6.2b.

a risk of invasion of privacy and 100% of these Internet café owners identified “incorrect logouts” by the clients as the main factor responsible for enhancing invasion of privacy.¹²⁷

From the research it also emerged that the customers in Internet cafés typically fell into one of the following 2 broad categories;

(1) Skilled internet users, who required little or no assistance to log on to the Internet to access information and access their mail. About 30% of the customers questioned/or observed in Nigeria and 70% in South Africa fell into this category.

(2) Unskilled or semi-skilled users, who required assistance to access information on the Internet and/or to retrieve their mail. About 70% of the customers observed in Nigeria and 30% in South Africa needed help to download information or send messages at some stage during their transaction time.¹²⁸

It was observed that in assisting the unskilled or semi-skilled Internet users, Internet café owners or their employees were physically present and were able to see the customer’s password and the information being processed. The potential misuse of personal information acquired by Internet café workers while assisting customers, as well as the possibility of using customers’ passwords for unauthorised access to personal information (in the customers’ absence) is another identifiable threat to customers’ privacy.

¹²⁶ Cf Appendix at Para 1.6.1a.

¹²⁷ Cf Appendix at Para 1.6.2a.

It is however anticipated that as users become more familiar with the technology through consistent use, and with the rapid urbanisation rate in Nigeria, there will be more skilled computer and Internet users resulting in a decrease in the need for assistance in Internet cafes. However, while this may reduce the potential for invasions of privacy by such 'third party helpers', the risk inherent for the few remaining unskilled users cannot be ignored.

Closely related to the above, another way in which Internet cafes present a threat to privacy is the practice whereby internet café owners or their employees download and print mail on behalf of customers. Both in Nigeria and South Africa in 2003, it was observed that it was deemed standard practice for mail to be downloaded and printed on behalf of both the skilled and unskilled Internet café users.¹²⁹ Such access to information by others carries with it the risk of misuse. While 25% of the Nigerian Internet café users recognising the threat to privacy caused by Internet cafes identified such download as one of the ways in which privacy could be invaded, it is noteworthy that none of the South African users or owners made reference to this practice.¹³⁰

Yet another factor posing a potential threat to personal privacy is the environment and physical/structural set-up of some of the Internet cafes visited. It was observed that some

¹²⁸ Ibid.

¹²⁹ Where a customer opened an e-mail account through an Internet café, if that customer's mail accumulated due to neglect over a given period of time e.g. three weeks, the Internet café owner would print out such mail on behalf of the customer at that customer's expense. Such mails were then deleted to free up space on the computers.

¹³⁰ It is possible that this practice is more common in Nigeria than in South Africa.

of the businesses were set up such that the Internet stations were located away from customer traffic in the room and the Internet station had dividing panels between them, giving some measure of privacy.

On the other hand, there were Internet cafes where no cubicles were available for Internet café users and the rooms were not sufficiently spacious. In this case, other customers or persons walking by the stations in the room could see information displayed on the monitors and, without much effort, read the information being processed by other customers. In Nigeria, 90% of the Internet café users who thought the use of Internet cafes posed a threat to privacy gave the example of peeping passers-by as a way in which privacy could be invaded.¹³¹ In South Africa only 17% of such Internet café users mentioned the possibility of invasion of their privacy in Internet cafes by peeping toms.¹³²

Further to this, it was observed that in all the Internet cafes visited, services other than Internet access were provided within the Internet café premises. These included in all cases, photocopying and public telephone services, and in some cases, the sale of stationery such as envelopes, pens, exercise books as well as cellular phone accessories and snacks. As such, customers came within the café premises for reasons other than

¹³¹ Cf Appendix at Para 1.6.1b.

¹³² Cf below Appendix at Para 1.6.1a. It was observed that clients using the computers in the Internet cafes visited in South Africa were provided with private or semi-private cubicles restricting access to the computers, while only one of the Internet cafes visited in Nigeria had this facility. In most cases, the computers in Nigeria were set up in an open room without any significant physical structure restricting traffic or access to the computers such that passers-by as well as other computer users could see/read what was on the other monitors situated close to theirs'.

Internet use and any of these customers could see or read information being processed on the computers without much effort. Such provision of other services on Internet café premises to the public widens the range of and gives license or access to a larger number of potential privacy invaders.

In Nigeria, further examples derived from the questionnaire of ways by which privacy might be invaded in Internet cafes included customers receiving mail through a third party address, hacking into others' passwords and mails and other technical means by which Internet café owners and others could access previously visited websites.

Personal information may also be wrongfully used or processed in Internet cafes by a third party, who is not the Internet café owner, or an agent thereof. In this case, depending on the facts and circumstances of the case, the Internet café owner may be able to bring an action against the third party.¹³³

All the Internet café owners interviewed in Nigeria indicated that they were aware of the threats to privacy occasioned by the use of Internet cafes.¹³⁴ In all cases, incorrect logouts by customers and third- party hacking were the first two identified causes by Internet café owners.¹³⁵ As in Nigeria, all the Internet café owners interviewed in South Africa recognised the threat to electronic mail and, or, Internet privacy posed by incorrect client

¹³³ For instance, an action for the tort of trespass may lie against an intruder who enters the premises of an Internet café owner in Nigeria unlawfully in order to wrongfully obtain information.

¹³⁴ Cf below Appendix at Para 1.

¹³⁵ Ibid.

logout and by hackers.¹³⁶

The above establishes that, although Internet cafes provide customers a much-needed means of communication, certain aspects of their use place customers at risk of having their privacy invaded. Moreover a number of Internet café owners and users (in Nigeria and South Africa) are aware of some of these risks.

1.5 The Need for a Re-examination of the Privacy and Data Laws in South Africa and Nigeria

The Constitutions of South Africa,¹³⁷ Nigeria¹³⁸ and those of many other Civil Law and Common Law countries recognise the right to privacy explicitly, thus providing a basis for its protection.¹³⁹ In South Africa (and other Civil Law countries),¹⁴⁰ the Civil Law provides a firm basis for the recognition of the right to privacy.¹⁴¹ The broad principles of the law of personality contained in the South African law of delict have hitherto been

¹³⁶ Ibid.

¹³⁷ Constitution of the Republic of South Africa, Act 108 of 1996.

¹³⁸ 1999 Constitution FRN.

¹³⁹ "Many countries in the world recognise a right to privacy explicitly in their Constitutions. At a minimum, these provisions include rights of inviolability of the home and secrecy of communication." See David Banisar & Simon Davies "Privacy and Human Rights: An International Survey of Privacy Laws and Practice" (1999) <http://www.gilc.org/privacy/survey/intro.html> Accessed September 2000. See also McQuoid-Mason in Chaskalson et al op cit at 38-19.

¹⁴⁰ For instance, Scotland, Germany, France, the Netherlands and Poland. See generally McQuoid-Mason op cit at 10, 57 & 74.

successful in giving protection in respect of many of the invasions of privacy that may be experienced in modern society, other than those by data banks.¹⁴²

Under Criminal Law as well, certain forms of invasion of privacy have been recognised as criminal wrongs.¹⁴³ The present Constitution of South Africa also makes provision for the right to privacy.¹⁴⁴ As for data, the Constitution does not have specific provisions protecting data. On the contrary, it provides for a right of access to information.¹⁴⁵

Presently, data protection legislation in South Africa is limited to the provisions of the National Credit Act¹⁴⁶ which protects credit information, the Statistics Act,¹⁴⁷ which protects, mainly information kept by government agencies (statistics), the Income Tax Act,¹⁴⁸ which protects information held by income tax officials in relation to their duties, and certain provisions of the Access to Information Act.¹⁴⁹ In addition, there is a proposed Consumer Protection Bill¹⁵⁰ which contains extensive provisions for the

¹⁴¹ See below Chapter 4.

¹⁴² See generally McQuoid-Mason in Chaskalson et al op cit at 18-4ff.

¹⁴³ Ibid.

¹⁴⁴ Act 108 of 1996, Section 14.

¹⁴⁵ Act 108 of 1996, Section 32.

¹⁴⁶ No 34 of 2005.

¹⁴⁷ Act 66 of 1976.

¹⁴⁸ Act 58 of 1962.

¹⁴⁹ Act 2 of 2000. Sections 30, 34-43, 61, 63-69 and a few other general provisions.

¹⁵⁰ Government Gazette no 28629; 15 March 2006.

protection of consumer information. Most significantly, there is a draft Data Protection Act¹⁵¹ that is expected to come into force in South Africa in the near future.¹⁵² The proposed South African Data Act will be examined in greater detail below.¹⁵³

In Nigeria, the Common Law of tort is based on English law of tort and there is no Common Law right of privacy.¹⁵⁴ There is a notable dearth of English Common Law cases on invasion of privacy, except for recent authority¹⁵⁵ decided on the basis of the Human Rights Act.¹⁵⁶ Although the Nigerian Constitution¹⁵⁷ makes provision for the protection of the right of privacy,¹⁵⁸ and previous Constitutions also contained provisions on the right to privacy,¹⁵⁹ thus providing a good basis for the protection of this right, this area of the law has not been considered much by the courts.

¹⁵¹ Project 124. See South African Law Reform Commission Issue Paper 24 “Privacy and Data Protection” at wwwserver.law.wits.ac.za/salc/issue/issue.html.

¹⁵² Cf below Para 7.1.2.2.

¹⁵³ Ibid.

¹⁵⁴ Now the English courts are bound to recognise and protect the right to privacy contained in the Human Rights Act of 2001. See below Chapter 3.

¹⁵⁵ See below Chapter 3.

¹⁵⁶ Chapter 42 of 1998.

¹⁵⁷ 1999 Constitution FRN.

¹⁵⁸ Section 37.

¹⁵⁹ Section 34, 1979 Constitution FRN and Section 36 of the 1989 Constitution FRN proposed during one of Nigeria’s military governments. The 1989 Constitution never came into force as that military government was removed in a *coup-d’etats* before the proposed date for the Constitution’s coming into effect.

Some protection for the right to privacy may be found under certain of the Common Law torts that protect rights analogous to the right to privacy in Nigeria.¹⁶⁰ Protection of the right to privacy may also be gleaned from other provisions in the laws of Nigeria,¹⁶¹ but generally, the right to privacy has received very little attention in Nigeria in terms of litigation and judicial interpretation. Data protection legislation is also lacking. In Nigeria, there is an obvious need for re-appraisal of the data laws.

The Constitutions of a number of African countries either refer expressly to the Universal Declaration of Human Rights as being applicable to their citizens, or contain detailed provisions on many of the rights proclaimed in the Declaration.¹⁶² The Universal Declaration of Human Rights recognises certain rights as ‘natural rights’, and specifically mentions the right to privacy in Article 12.

It is noteworthy that the African Charter on Human and People’s Rights¹⁶³ does not contain any direct provision on the right to privacy. This may be an indication of the

¹⁶⁰ For instance, the torts of trespass, nuisance, and others, as will be seen below, Chapter 6.

¹⁶¹ For example, the Criminal Code Act, Cap 77 LFN 1990, and the Evidence Act, Cap 112 LFN 1990; See below Chapter 7 for details.

¹⁶² The Constitutions of Ethiopia (Article 13, Constitution of the Federal Republic of Ethiopia 1994), Rwanda (Preamble to the Rwanda Constitution adopted 1995), Burundi (La Constitution de la Republique du Burundi Promulgue le 13 mars 1992 ainsi que Decret- loi no 1/001/96 du Septembre 1996), Cameroon (La Constitution du Cameroun Loi no 96-06 du 18 Janvier 1996), (in the preambles) among others, affirm their devotion and adherence to and provide for compliance with the principles and ideals of the Declaration. The Constitution of Angola (Constitutional Law of the Republic of Angola 1992) expressly provides for the inviolability of the home and secrecy of correspondence in Article 44 and provides for respect of the human person and human dignity, protection of personal integrity, good name and reputation as a well as free development of personality (Article 20). Similarly, the Constitution of Uganda (The Constitution of the Republic of Uganda 1995) guarantees the right to privacy of person, home and other property (Section 27). Namibia (Article 13) and Mozambique (Article 64) also have Constitutional provisions protecting privacy.

¹⁶³ African [Banjul] Charter on Human and People’s Rights, adopted June 27, 1981, O.A.U. Doc. CAB/LEG/67/3 rev.5, 21 I.L.M. 58 (1982) entered into force Oct 21, 1986.

importance that Africans generally have attached to the right to privacy. The African Charter does, however, guarantee certain rights that may be construed as protecting aspects of privacy, such as the right to integrity of the person,¹⁶⁴ the right to respect of the dignity of the person,¹⁶⁵ the right to liberty and the security of the person.¹⁶⁶

In the United States of America, although there is no specific provision for privacy in the Constitution, the Constitution forms the basis for the recognition of the right to privacy, relying on the provisions of the First, Third, Fourth, Fifth, Ninth and fourteenth Amendments.¹⁶⁷ Similarly in Germany, although it is not specifically mentioned in the Constitution, the law of privacy is protected by the German Basic Law in the articles dealing with dignity,¹⁶⁸ the right to self-determination,¹⁶⁹ the privacy of posts and telecommunications¹⁷⁰ and the inviolability of the home.¹⁷¹

In 1994 the French Constitutional Court ruled that the right of privacy was implicit in the Constitution.¹⁷² Prior to 1970, the French courts had recognised a right to privacy, which

¹⁶⁴ Article 4.

¹⁶⁵ Article 5.

¹⁶⁶ Article 6.

¹⁶⁷ See Douglas J in *Griswold v Connecticut* (1965) 381 U.S. 479 at 484.

¹⁶⁸ Article 1.1.

¹⁶⁹ Article 2.1.

¹⁷⁰ Article 10.

¹⁷¹ Article 13.

¹⁷² 94.352 Dc.

was among the strongest in the world.¹⁷³ The tort of privacy was first recognised in France in 1858.¹⁷⁴ As for data protection, the French Data Protection Act was enacted in 1978.¹⁷⁵ In Germany, the first data protection law was passed in the Land of Hesse in 1970¹⁷⁶ and the Federal Act on Data Protection was enacted in 1977.¹⁷⁷

Many of the above laws protecting privacy and data preceded the current explosion of information technology and have been revised accordingly. Presently, the dangers of surveillance of the individual and potential invasions of privacy with the advancement of technology have reached enormous proportions.

In terms of easy access to vast information and data and the capability to publish or disclose such information, technology appears to have “outpaced the legal protection of privacy” in the more technologically advanced countries, over a decade ago.¹⁷⁸ As a result, there is no foolproof method or technology to safeguard information stored in data banks or to prevent access to, or publication of information via the Internet.¹⁷⁹

¹⁷³ For instance, a statute of 11 May 1868 criminalized the publication of any fact relating to private life (Article 11); See also McQuoid-Mason *The Law of Privacy in South Africa* op cit at 73.

¹⁷⁴ The Rachel affaire, Judgement of June 16, 1858, Trib. Pr. Inst. De la Seine, 1858 D.P. 111 62.

¹⁷⁵ Loi Ni 78-17 du Janvier 1978 relative a l’informatique, aux fichiers et aux libertes. Journal officiel du 7 Janvier. See generally Banisar & Davies op cit.

¹⁷⁶ See Banisar & Davies op cit at <http://www.gilc.org/privacy/survey/surveyak.htm/#Germany>.

¹⁷⁷ Ibid. The Federal Act on Data Protection (27 January 1977) was reviewed in 1990. See <http://www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm>

¹⁷⁸ See Sloan op cit at 4.

¹⁷⁹ Cf above at 12, 13, 18-20. See also Sloan op cit at 5.

There is a need constantly to re-appraise privacy and data protection laws to bridge the gap between technology and the law if society is to avert possible privacy anarchy. Unless urgent and effective measures are taken, the gap may increase to the extent that the task of bridging it becomes almost impossible. In many advanced and technologically developed countries, there have been efforts to rise to the challenge of the changing times, and laws have been passed to keep up with developments in modern society.¹⁸⁰

1.6 Privacy and Data Protection in South Africa and Nigeria

This work focuses on South Africa and Nigeria for a number of reasons. South Africa is one of the best- developed countries in Africa in terms of technology, and it has a population consisting of people of different colours and cultures. Nigeria on the other hand, is not as technologically advanced as South Africa. It however has the largest population of people in Africa, and is the most populous black nation on earth. Both countries therefore provide a suitable basis for assessing the practice in Africa and for comparing and contrasting the situation within Africa.

It is suggested that the ideas of privacy of the black man, or woman may, differ from those of persons of other colour, cultures and background. In this regard, as previously noted, the African Charter does not contain a provision on the right to privacy, and many

¹⁸⁰ For instance, in the United Kingdom, where the Common Law of England did not recognise a right to privacy until the recent adoption of the Human Rights Act of 2001, which now contains provision on the right to privacy. The data protection laws of the United Kingdom were also revised in 1998. See below Chapter 3.

of the African countries that do have provisions on the right to privacy have imported it from the Universal Declaration of Human Rights.¹⁸¹

It must be noted that although privacy has been described as an amorphous concept,¹⁸² it is not an abstract concept. However, its definition can only be accurate when viewed within the context of the specific people, society and time in which it is being discussed.¹⁸³ In this regard, it has been observed that privacy has become an issue in “modern democratic societies, which are characterised by large- scale sophisticated bureaucratic structures and advanced technology in communications and information systems”.¹⁸⁴

In this light, it is suggested that Nigeria’s black population and level of technological advancement are relevant to the state of the law of privacy in the country. With regard to technology, Nigeria is developing and is still in need of infrastructure to support effective

¹⁸¹ For example, the Constitutions of Algeria (1996), Burundi (1992), Cameroun (1996), Mozambique (1990), Namibia (1990), Niger (1991), Rwanda (1995) and many others.

¹⁸² Cf above at 1.

¹⁸³ See Sloan op cit at xiii “Privacy is virtually impossible to define in strictly legal terms. It varies with the times, historical context, the state of the culture and the prevailing judicial philosophy.” Cf G.S.McCellan *The Right to Privacy* (1976) at 25 where he states that privacy can only be defined in relation to a national culture, a particular political system and a specific period of time. For instance, the Constitution of the United States of America did not originally include a right to privacy, but because of the changes in society and the need to “reinterpret democratic values in changing social context” the state of California amended its Constitution to include the right to privacy as a fundamental right. See also Reed op cit at 227.

¹⁸⁴ Ibid; See also P O’ Higgins *Cases and Materials on Civil Liberties* (1980) at 345: “[T]he scope of privacy is governed to a considerable extent by the standards, fashions and mores of the society ... and these are subject to constant change... ”.

large-scale use of some of the technological devices that are commonplace in developed countries.¹⁸⁵

Regarding Nigeria's black population, in the cultures of the different tribes,¹⁸⁶ even though a person's individuality is acknowledged¹⁸⁷ socially, individuals are defined and exist in relation to family and community. Nigeria consists of close-knit family institutions and small communities where one's privacy is invariably shared with the family. No one exists as an island and popular acceptance prescribes that a person "is his brother's keeper."¹⁸⁸

In such a collectivist society,¹⁸⁹ certain acts that might be perceived as invasions of privacy, or grossly offensive to persons in an individualistic¹⁹⁰ society would not be regarded as serious or wrong.¹⁹¹ On the strength of this, it is suggested that cases of invasions of privacy by "peeping toms" in the Nigerian society, particularly, those

¹⁸⁵ For instance, Closed- Circuit Television cameras and Automated Teller Machines.

¹⁸⁶ Yoruba, Ibo, Hausa mainly, and various other tribes and people e.g. the Benin people, the Fulani, Efik, Ijaw, Itshekiri. O.Otitie "Nigeria's Identifiable Ethnic Groups" <http://www.onlinenigeria.com/tribes/> Accessed January 2006.

¹⁸⁷ F Oyedeji "The Influence of Natural Law on the Nigerian Legal System" (1998) (unpublished LL.M thesis) at 74.

¹⁸⁸ Ibid.

¹⁸⁹ P Anderson "Explaining Intercultural Differences in Nonverbal Communication" in L A Samovar & R E Porter (eds) *Intercultural Communication: A Reader* (1994) 232-234.

¹⁹⁰ Ibid.

¹⁹¹ Anderson in Samovar & Porter op cit at 233-234.

occurring prior to the information technology age, might not have been considered sufficiently grievous to warrant legal action.¹⁹²

This is relevant for our purpose because case law has demonstrated that laws are better - observed and more effective where the people for whom they are made can relate to them.¹⁹³ In essence, for our purpose, in considering the evolution or development of the law of privacy, this knowledge may partially explain the relatively underdeveloped state of the law of privacy in Nigeria and it may also be useful in suggesting provisions for a law of privacy for Nigeria, in deciding what to adopt, adapt or reject from other legal systems.

With regard to Nigeria's state of development and socio-cultural situation, towards the late 1990's, there has been an increased usage of the Internet, electronic mail, facsimile and other technological equipment. With urbanisation,¹⁹⁴ transactions that formerly

¹⁹² Cf Anderson in Samovar & Porter op cit at 233-234. Where a person was seriously aggrieved by the action of a peeping tom, it would be possible to bring an action for invasion of privacy under the Constitution (Section 34 Constitution FRN 1979, Section 37 Constitution FRN, 1999); or at Common Law, where the wrongful act involved the commission of a tort e.g. trespass, nuisance.

¹⁹³ For example the Nigerian Public Health Act (Cap 165 LFN 1958) prohibits the slaughtering of animals except under certain specified conditions, including the obtaining of a license. However, under the various local customs, animals are killed for food to mark certain special occasions e.g. puberty, home-coming, weddings and during the festive seasons like Christmas, Easter and Ramadan. In these cases, it is common for families to kill animals for food to share with friends and family. It is also common to keep chickens, goats, sheep and other livestock for food, where there is space around the house. Cap 165 of 1958 is honoured more in its breach than in its observance. Various State laws also prohibit setting fire to or burning bushes (e.g Ondo State Edict No 4 of 1989) and provide stiff penalties for the offence. However, this has not deterred farmers and hunters who engage in this practice and bush burning still thrives among them. Cf D A Ijalaye "The Sociological School of Jurisprudence and the Nigerian Legal Order" (1992) in *Nigeria and the Challenge of Knowledge (Essays in Honour of Jonathan Olusesan Dipeolu)* 33 at 35ff.

¹⁹⁴ In 2000, Nigeria was 44% urbanised, with the level of urbanisation reported to be increasing rapidly. W Erickson, T Lloyd-Jones, M Theis, I Greatbatch, B Mulyawan, M B Yunusa, S Adenekan, A Hasan, C Monteiro, N Dantas, F Sobriera, M Batty "Mapping Urbanisation for Urban and Regional Governance"

required personal contact can now be done electronically, without necessitating physical contact, and the extended family and the community have a reduced hold on an individual's affairs and on his or her private space. On the other hand, many modern day electronic communication facilities, for instance, e-mail, are only available to the individual through internet cafes or other public, or semi-private means (for instance computers in the workplace), thereby creating a potential means of invasion of privacy by others using the same system.

As in Nigeria, South Africa's population of people of different colour and cultures, coupled with the advanced technology available in South Africa, are relevant to the state of the development of the law generally, and its law of privacy particularly. While Nigeria suffered under military rule, South Africa was subjected to autocratic minority rule.

Furthermore, in comparing, and drawing inferences with regard to the law of privacy in Nigeria and South Africa in this work, it is notable that both countries share similarities in their history of governance. In Nigeria, in spite of the fact that several Constitutions have guaranteed the right to privacy,¹⁹⁵ for more than thirty out of its forty years of independence, Nigeria has been under military rule, which has been characterised by a

(2003) Final report 2003 DFID Research R8130, Max Lock Centre, University of Westminster at 5.
http://www.wmin.ac.uk/builtenv/maxlock/mapping/Report_for_Web/Word_final/1_Summary_MU.doc.
Accessed March 2006.

¹⁹⁵ Section 34, 1979 Constitution FRN; Section 36, 1989 Constitution FRN; Section 37, 1999 Constitution FRN.

general disregard of the human rights provisions in the Constitution,¹⁹⁶ and gross violations of the civil rights of the citizens by the army.¹⁹⁷

Although Constitutions that provided for human rights, including the right to privacy, were proposed during two of the military regimes,¹⁹⁸ the right to privacy received little or no attention during military rule. Several years after the end of military rule and with the establishment of democracy, there has still been very little litigation and judicial interpretation of the Constitutional provision on privacy, and thus minimal development of the law of privacy.

In South Africa, although under the autocratic rule of the minority apartheid regime there were gross violations of human rights, there was a common law right to privacy, which was recognised and upheld by the courts.¹⁹⁹ South Africa has a democratic Constitution

¹⁹⁶ For instance, on assumption of power, each military Government promulgated a Constitution (Suspension and Modification) Decree, (e.g. No 1 of 1966 and No 1 of 1984), which in effect suspended the Constitution and made its provisions subject to their Decrees (which were usually made arbitrarily). Thus they had unfettered power and none of their actions could be challenged as unconstitutional.

¹⁹⁷ E.g. under the State Security and Detention of Persons Decree (No 2 of 1984), private homes were arbitrarily searched and people were often detained and left in detention without trial. In *Gloria Mowarin v A.G. of the Federation* (Unreported; see *The Guardian* February 20, 1991 pp 1-2), the plaintiff was detained by the Vice President under Decree 2 of 1984 and Decree 24 of 1990, which gave the Vice President certain powers. However, at that time, the office of the Vice President did not exist. The court held that the detention was illegal and termed Decree no 24 a "legislative absurdity". See also *Lakanmi v A.G. of Western State & others* (1971) UILR 20.

¹⁹⁸ The 1989 Constitution of the Federal Republic of Nigeria was introduced under General Ibrahim Babangida's military rule, but that regime was overthrown in a military *coup d'etats* before the Constitution could come into force. Section 36 of the proposed 1989 Constitution guaranteed the right to privacy. Similarly, in the 1993 Constitution proposed under General Sanni Abacha's military rule, Section 37 recognises and provides for the right to privacy.

that emphasises human rights and includes the right to privacy. The history of the disregard of human rights in both countries is a point of similarity, which may be relevant in suggesting a similar approach in both countries, to improving the law protecting privacy.

A comparative analysis of the laws of privacy and data protection in South Africa and Nigeria will be made in this work against a brief discussion of developments in the United Kingdom, the United States of America and Germany. Since these are developed nations in terms of technology, it is believed that their privacy and data protection laws will to a degree be reflective of current technological development. As such, they will be instructive in South Africa, which is itself a developed nation. Moreover, the courts in South Africa must follow precedents from public international law²⁰⁰ and may refer to other jurisdictions with similar provisions in their Constitutions,²⁰¹ including the United States of America²⁰² and Germany.²⁰³

The choice of Germany in particular is informed by the fact that Germany, like South Africa, has a Civil Law system (unlike the United States and the United Kingdom). Cases

¹⁹⁹ See *Gosschalk v Rossouw* 1966 (2) SA 476 (C) at 492, *S v A* 1971 (2) SA 293 (T), *Reid-Daly v Hickmann & others* 1981 (2) SA 315 (ZA) at 323. See generally McQuoid-Mason in Chaskalson et al op cit at 1-4.

²⁰⁰ Section 39(1)(b), Constitution of the Republic of South Africa (Act 108 of 1996) See also *Bernstein v Bester* NO 1996 (2) SA 751 (CC) at 790ff.

²⁰¹ Section 39(1)c, Constitution of the Republic of South Africa (Act 108 of 1996).

²⁰² See Ackermann J in *Bernstein v Bester* supra at Para 75.

²⁰³ See Ackermann J in *Bernstein v Bester* supra at Para 77ff.

and trends in the development of the law in Germany and South Africa may thus be juxtaposed for better enlightenment on Civil Law. Nigeria on the other hand, has a Common Law system and follows precedents from English law,²⁰⁴ public international law²⁰⁵ and other jurisdictions with similar provisions in their constitutions.²⁰⁶ The laws in Germany, the United Kingdom and the United States may thus give more guidance to developments in South Africa and Nigeria.

Notably, the constitutions of Germany and the United States do not make specific provision for the right to privacy but a right to privacy has been recognised and developed in these two countries. Also, the United Kingdom does not have a written Constitution and has only recently recognised a right to privacy., Nigeria

This work is not an exhaustive analysis of the state of the privacy and data protection laws of the United Kingdom, the United States of America, or Germany; the laws in these jurisdictions are merely used for comparative purposes. The focus of this research, as previously indicated,²⁰⁷ will be the privacy and data protection laws of South Africa and

²⁰⁴ Section 45 Interpretation Act (Cap 192 LFN 1990). In *Abiola v Ijoma* [1970] 2 All NLR 268 at 272, Dosunmu J relied on the English Common Law principles relating to the protection of individuals regarding the tort of nuisance and also cited the opinions of certain English judges (Lord Halsbury, Lord Loreburn, Luxmoore J); See also generally D Olowu & F Laosebikan "Sources of Law in Nigeria" in A O Sanni (ed) *Introduction to Nigerian Legal Method* (2006) at 245-249.

²⁰⁵ Section 12(1) 1999 Constitution FRN; See also Olowu & Laosebikan in Sanni op cit at 129.

²⁰⁶ For instance, the Nigerian courts have relied on Ghanaian cases in establishing the essentials of the tort of malicious prosecution. See *Inneh v Aruegbon* (1952) 14 WACA 73; *Aubin v Ehunaku* [1960] GLR 167; *Soadwah v Obeng* [1966] GLR 33; See also G Kodilinye *The Nigerian Law of Torts* (1982) at 26ff. [Newer version available G Kodilinye & O Aluko *The Nigerian Law of Torts* (1999)]

²⁰⁷ Cf above Para 1.3.

Nigeria, with particular reference to electronic mail use in Cyber/Internet cafes. As mentioned above,²⁰⁸ today, the use of the internet is commonplace in many countries including South Africa and Nigeria and many internet users in South Africa and Nigeria do not own or have ready access to private computers.²⁰⁹

1.7 Conclusion

In this research work, the impact of the cyber revolution will be considered, generally showing the ways in which South Africa and Nigeria have been affected, after which the privacy and data protection laws of the United Kingdom, the United States of America and Germany will be examined. Next, the privacy and data protection laws in South Africa and in Nigeria will be considered. What are these laws? How have they been developed to meet current challenges? Are these laws adequate or effective to protect privacy and data with regard to information processed in Internet cafes? Do they serve as a deterrent to would-be invaders of privacy? Do they provide sufficient remedies? These issues will be evaluated.

Having comparatively examined the laws in these countries, and having made an evaluation of their effectiveness, recommendations for privacy and data principles/provisions that will provide protection for information processed in Internet cafes in South Africa and Nigeria will be made.

²⁰⁸ Cf above at 19ff.

²⁰⁹ Cf above at 14 ff.

CHAPTER TWO

THE EFFECT OF INFORMATION TECHNOLOGY AND THE CYBER REVOLUTION ON SOUTH AFRICA AND NIGERIA

2.1 Introduction: Evolution and Development of the Computer

The computer has been around for over a century,²¹⁰ but its effect on law and the society today cannot be over-emphasised. The computer was initially just a device for calculating figures (numbers), but since its original appearance there have been modifications and improvements to it, that have reached unimaginable heights.²¹¹ Today, the computer is not only a computational machine but also a communication device.²¹² It processes and transmits data, it stores and retrieves information and is, to a large extent, an information device.

There are many ways in which the computer has impacted on the world²¹³ and changed the pattern of transactions, work, and life in general in the last two decades. Data banks and computerised pools of information, surveillance devices, especially the ubiquitous closed-circuit camera, identity systems, biometrics and the Internet, are some of the

²¹⁰ R M Baer *The Digital Villain* (1972) at 35 ff.

²¹¹ Cf Baer op cit at 35ff.

²¹² S Nora & A Minc *The Computerisation of Society* (1981) at vii.

²¹³ See I J Sloan *Law of Privacy Rights in a Technological Society* (1986) at 23. Sloan notes that: "Computers are used for controlling traffic lights ... making hotel and motel reservations, maintaining hospital records, monitoring patients with severe heart problems, storing financial information ...".

technological advancements that have made an impact on the world. Computers in internet café are used for access to information, communication via e-mail and simple typing and printing jobs. In carrying out any of these tasks, information relating to the user is processed and at least a part of the processed information is retained in the memory of the computer. It is intended in this chapter to examine some of the contemporary technological devices and their impact on the right to privacy and the protection of personal data.

2.2 Development of Information Technology and its effects on the right to privacy

This section will examine some of the technology facilitating invasions of privacy where such technology is directly relevant in considering the issue of invasion of electronic mail privacy in Nigeria or South Africa, or where such discussion is necessary or desirable to provide a fuller context within which to discuss electronic mail privacy.

2.2.1 Data banks and computerized pools of information:

Data banks store, recall or search for stored information using the computer's memory. Any kind or variety of information such as records of births, deaths, marriages, medical information and records, financial and insurance records, criminal records and even personal facts such as characteristics, reputation of individuals may be stored.²¹⁴ Legal

citations, market research materials, census data, data for economic, urban planning and the like can also be processed and retrieved easily through these information banks.²¹⁵

Data processing networks are also used to register purchases in stores through computer terminals. Orders for goods can also be placed and processed electronically. In addition, invoices and inventories are frequently controlled through computer programs. In a broad sense, “much paper work has been replaced by an electronic transfer system.”²¹⁶

Data banks are extremely useful. Generally, they facilitate access to the total accumulation of information.²¹⁷ In addition, social, economic, health and other issues, demographic aspects of disease, unemployment, and many other issues affecting human life and well-being may be better researched with the enormous reservoir of data made available through data banks.

Data banks are kept and utilised in nearly every department of government for the maintenance and retrieval of (accurate) records and statistics. They are also used for research purposes regarding health, census, environmental, urban and regional planning and in other areas of governmental conduct. Data banks and computerised pools of

²¹⁴ See D J McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 7ff; See also J Neethling *Neethling's Law of Personality* (2005) at 293-294.

²¹⁵ Nora & Minc op cit at ix.

²¹⁶ Ibid.

²¹⁷ See generally Baer op cit at 132-135.

information are utilised in most countries of the world, including South Africa and Nigeria.

Although not all computer systems qualify *stricto sensu* as data banks within the meaning above, it is arguable that where information (data) regarding a particular individual is accumulated on a specified computer system, such that it is possible to get a reasonable amount or quality of personal information about a person, to which a third party would not ordinarily have access, that computer system may, for our purpose, be regarded as a data bank. Thus, where they are regularly used and have accumulated in their memory personal information of a nature or quality that would not be ordinarily accessible to a third party, computer systems in Internet cafés may be regarded as some form of data bank.²¹⁸

Computers in Internet cafes are commonly used for typing and printing out curriculum vitae, student projects including long essays, term papers and theses. They are also used for sending and receiving personal as well as business e-mail and as such, may contain personal information, and business information. Such information when accumulated and retained in the computer's memory, would qualify as data,²¹⁹ and may be misused.

Regarding the threat that data banks pose to the privacy of individuals, the very fact of the existence of a data bank is a potential threat to personal privacy and freedom in the sense that personal information that could otherwise have been kept largely undisclosed

²¹⁸ Cf Section 1(1) of the United Kingdom Data Protection Act Cap 29 of 1998. Cf below Para 3.2.2.2.2.

²¹⁹ Cf below at 63.

and in the custody of the person concerned, is being kept centrally in a database. The information is thus removed from the hands of the owner and placed in the custody of computer users. Furthermore, as noted above,²²⁰ information gathered in a data bank may be accessed unlawfully²²¹ and may also be misused.²²² In addition, the information in data banks is not always accurate.²²³

In South Africa, although there are statutes that regulate information collected about individuals by the state and its agencies or departments,²²⁴ there is no data protection law or other law specifically made for the protection of information.²²⁵ The South African Law Commission is however working on a draft Data Privacy Act.²²⁶

The Promotion of Access to Information Act²²⁷ regulates information use and disclosure by both the public and private bodies in South Africa. In Nigeria, data banks are used by

²²⁰ Para 1.3.

²²¹ See Baer op cit at 134.

²²² Cf Sloan op cit at 6f; In *Menard v Mitchell*, 430 F.2d 486 (DC Cir 1970) a Federal district court in Washington, DC forbade the FBI from disseminating criminal history records for use in determining employment or licensing acceptability. The judge was of the opinion at that time, that “[n]o procedure exists to enable individuals to obtain, supplant, or to correct the criminal record information being used against them; ... control of the data will be made more difficult and opportunities for improper use will increase with the development of centralised state information centers”.

²²³ See Baer op cit at 134-135.

²²⁴ For instance, the Income Tax Act (No 56 of 1962, as amended by Act 19 of 2001), the Statistics Act (No 66 of 1976) as amended by Act No 6 of 1999). See below Chapter 7.

²²⁵ See Neethling op cit at 296; McQuoid-Mason op cit at 196-197. See also Roos op cit at 660ff.

²²⁶ See South African Government Information; Media Statement by the South African Law Commission Concerning Its Investigation into Privacy and Data Protection. <http://www.info.gov.za/speeches/2002> Accessed March 2007. Cf also Michalson’s Guide to Data Privacy Law in SA <http://www.michalson.com/docs> Accessed March 2007.

both private and government agencies, but there is no data protection law or body in Nigeria. However, there is legislation regulating the collection and publication of information by specific government departments or agencies, and these protect data or information collected by these bodies.²²⁸

2.2.2 The Internet

The Internet is an international or global “network of interconnected computers”,²²⁹ by which people around the world are linked across geographical boundaries. The Internet provides two major services, which have bridged the gap of geographic borders and revolutionised communication locally and internationally. The one is electronic mail, which allows for the sending and receiving of information or mail electronically anywhere in the world. Mail so sent is received within seconds or a few minutes of being sent.

The other service offered by the Internet is the world wide electronic media, known as the World Wide Web. It is a public “notice board” containing an almost inexhaustible range of information that virtually the whole world can access; read from, or write to as long as

²²⁷ No 2 of 2000 as amended by No 54 of 2002. See below Chapter 7. The data protection provisions in the original draft Bill were unused and a separate Act will have to be passed to cover data protection.

²²⁸ For instance, The Income Tax (Authorised Communications) Act (Cap 175 LFN 1990) contains provisions regulating the obtaining and disclosure of tax-related information; and the National Population Commission Act (Cap 270 LFN 1990) contains provisions regulating the obtaining and disclosure of information by the Commission. See below chapter 7.

²²⁹ J H Lipshultz *Free Expression in the Age of the Internet - Social and Legal Boundaries* (2000) at 106.

they are connected to the network. It has also been referred to as “the information superhighway”.²³⁰

The accessibility and ease of use of the Internet highly increase the likelihood of abuse.²³¹ Moreover, the effectiveness of the Internet in terms of speed and reliability with which information can be published facilitates widespread and even universal publication or disclosure. Generally in these ways, the Internet constitutes a potential threat to the right to privacy. In addition, and in particular, names and other personal details of users are sometimes required to obtain access to certain websites or programs. They are also used to carry out purchase and other transactions on the Internet. Furthermore, Internet users are often watched in different ways for different reasons.²³²

In South Africa, the Internet is widely used in both private and government offices and in institutions of learning. Apart from this, many individuals and families have personal computers and often send and receive electronic mail via these systems. In the business world, computer-based transactions are fast increasing and Internet banking has become possible. To further facilitate communication, certain types of cellular phones may also be used to access the Internet.²³³

²³⁰ Lipschultz op cit at 10, 106.

²³¹ See Lipschultz op cit at 10: “The Internet is both a ‘broadcast’ and ‘common carrier’ medium ... [where] ... individuals have the power to be their own publishers. The openness of the technology increases the possibility that information will be disclosed regardless of whether it is right or wrong ... anyone can be a publisher of something that looks like a newspaper. Secondly, online information is non-standard and can be distributed anonymously.”

²³² For example, ‘cookies’ may be used to monitor ‘surfers’ and obtain other details about them and consumers may be watched to determine their tastes. See above Para 1.2.

In Nigeria, the Internet is also used in government departments, private companies, business concerns and banking institutions. Even though only a small percentage of individuals have personal computers, there is a proliferation of “cyber-cafes” where anyone may access the Internet, send and receive e-mail at little cost, and where information may be downloaded from the Internet.²³⁴ This is commonly used by a large number of students and workers who cannot afford to have personal computers, but need to be in contact with the outside world.²³⁵ The threat posed by the Internet to the right of privacy is one that affects both South Africa and in Nigeria.

2.2.3 Identity Systems

2.2.3.1 Identity Cards

Different forms of Identity (ID) cards are used in virtually all countries of the world.²³⁶ The type of card and its function may vary. It has been observed that in some countries, for instance Spain, Portugal and Singapore, identity cards have been linked to national registration systems to be used as the basis of government administration.²³⁷ It has also been suggested that race, politics, and religion were at the heart of older identity

²³³ Cf above Para 1.2.

²³⁴ Cf above Para 1.3. See also Segun Aregbeyen “Nigeria Lacks Legal Protection Against Piracy on the Internet” in *The Comet* October 25, 2000 at 22.

²³⁵ Cf above Para 1.3.

²³⁶ D Banisar & S Davies “Privacy and Human Rights: An International Survey of Privacy Laws and Practice” (1999) <http://www.gilc.org/privacy/survey/intro.html#defining> Accessed September 2000.

²³⁷ Ibid.

systems.²³⁸ With the advent of magnetic stripes and microprocessor technology, these cards can also become an interface for receipt of government services.²³⁹ Identity cards can thus be a means of identification as well as to provide access to social services.

While Germany,²⁴⁰ South Africa²⁴¹ and many developed countries,²⁴² have official compulsory national identity cards or books that are used for a variety of purposes, a considerable number of developed countries such as the United Kingdom, the United States of America, Canada, Ireland, Australia, and New Zealand do not have such cards.²⁴³ Until February 2003 when the issuing of identity cards began officially in Nigeria, Nigeria did not have an official identity system.

Where there is no national identity system in place, there are alternative methods of identifying oneself and establishing one's citizenship. In the United States for instance, every citizen of the country has a social security card. Through the social security

²³⁸ See J Torpey *The Invention of the Passport: Surveillance, Citizenship and the State* (2000) at 76, 97ff; see also D Banisar "Privacy and Human Rights" (2001) <http://www.privacy.org/pi/summary/phr2000/threats.html#heading2> Accessed October 2002. Cf D McQuoid-Mason *The Law of privacy in South Africa* (1978) at 159, 235, where he notes that Identity systems were used in South Africa during the apartheid regime under the Population Registration Act to identify different races.

²³⁹ Banisar & Davies (1999) op cit at <http://www.gilc.org/privacy/survey/intro.html#defining>.

²⁴⁰ *Gesetz über Personalausweise vom 21 April 1986*, BGBl. I, S. 548; Cf D P Currie *The Constitution of the Federal Republic of Germany* (1994) at 321.

²⁴¹ Identity Act No 68 of 1977 as amended by Identity Amendment Act No 28 of 2000.

²⁴² For instance France, Belgium and Greece. See generally Banisar & Davies op cit at www.gilc.org/privacy/survey/intro.html#defining.

²⁴³ See Banisar & Davies (1999) op cit at www.gilc.org/privacy/survey/intro.html#defining.

number, an enormous amount of personal information can be traced.²⁴⁴ In the United Kingdom, a “tradition of personal liberty”²⁴⁵ where citizens are not subject to internal checks or ID cards has been upheld.²⁴⁶

However, citizens of the United Kingdom have birth certificates, which are sometimes used as means of identification.²⁴⁷ Driver’s licenses may also be used for identification in the United Kingdom.²⁴⁸ There are however ongoing debates on the question of adopting national identity cards in the United Kingdom.²⁴⁹ In Nigeria, drivers licenses, work identity cards (issued by private companies, businesses, government departments and parastatal bodies), and student identity cards have been commonly used. The national passport may also be used for identification when outside the country.

The refusal to adopt or failure to have a national identity system in some countries has been done to protect human rights.²⁵⁰ It has been observed that the existence of national

²⁴⁴ See H Henderson *Privacy in the Information Age* (1999) at 21 & 22.

²⁴⁵ Alan Travis “ID Cards UN-British or Vital? The ID Debate” in *the Guardian* 25 September 2001 at <http://politics.guardian.co.uk> Accessed June 2003.

²⁴⁶ *Ibid.*

²⁴⁷ For instance, production of a valid birth certificate by a person born in Britain may serve as proof that such a person is a British citizen.

²⁴⁸ In traffic-related offences, drivers’ licenses are used for identification purposes.

²⁴⁹ See generally Privacy International “National ID Cards” (2002) <http://www.privacyinternational.org/issues/idcard/> Accessed November 2002; See also B Williams “Rulers Discuss Issuing National I.D. cards” in *The Militant* (2001) Vol 65 NO 39 at <http://www.themilitant.com> Accessed December 2002; Travis op cit.

²⁵⁰ See Williams op cit; Travis op cit.

identity documents appear to parallel increases in police powers.²⁵¹ The imposition of identity card systems has been successfully challenged on grounds of constitutional privacy in a number of countries.²⁵²

In 1991, the Hungarian Constitutional Court ruled that a law creating a multi-use personal identification number violated the constitutional right to privacy.²⁵³ In 1998, the Philippine Supreme Court ruled that a national identity system violated the constitutional right to privacy.²⁵⁴ In the United States of America, there is a strong opposition to a national identity card system.²⁵⁵ The American Civil Liberties Union is especially opposed to the idea on the grounds that it threatens the right to privacy and would create an easy tool for government surveillance.²⁵⁶

In South Africa, the Identity Card system was in place under the apartheid regime and it was essential for voting. Although the police could commit numerous invasions of

²⁵¹ Identity Cards were abolished in Britain in 1953, following a court ruling that the police powers that went with them, which included the power to stop citizens at random and require that they present identification, created an undesirable situation between the people and the government. See Williams op cit; See also Banisar & Davies op cit at <http://www.gilc.org/privacy/survey/intro.html#defining>.

²⁵² ACLU "National Identification Cards: Why Does the ACLU Oppose a National ID Card System?" (1996) <http://www.aclu.org/library/aaidcard.html> Accessed November 2001; ACLU "National ID Cards: 5 Reasons Why They Should Be Rejected" http://archive.aclu.org/issues/privacy/National_ID_Feature.html (2002) Accessed June 2003.

²⁵³ Constitutional Court Decision No 15 AB of 13 April 1991.

²⁵⁴ Philippine Supreme Court Decision of the National ID System, July 23, 1998, G.R. 127685 (1998) <http://bknet.org/laws/nationalid.html> Accessed February 2000.

²⁵⁵ EPIC "National Identity Cards" http://www.epic.org/privacy/id_cards/default.html (2002) Accessed November 2002.

²⁵⁶ See ACLU op cit at <http://www.aclu.org/library/aaidcard.html>.

privacy, by virtue of certain laws, under the apartheid regime,²⁵⁷ with the institution of a democratic government and Constitution, this is no longer the case.

The powers of the police and other security agencies must be exercised in accordance with the Constitution, which expressly provides that national security must be pursued in compliance with the law, including international law,²⁵⁸ and that the security services (which includes the police services, defence force and intelligence services) and their members must act “in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic.”²⁵⁹ In the light of this, acts that would be an infringement of human rights generally and the right to privacy particularly are outlawed.

In March 1998, the South African Cabinet approved a plan to issue a multi-purpose smart card that combines access to all government departments and services with banking facilities. In the long term, the smart card is intended to function as a passport, driver’s license, identity document and bankcard.²⁶⁰ It is noted that when this comes into effect, there will be greater possibilities for invasion of privacy, as the card would allow access

²⁵⁷ For example, the Internal Security Act 74 of 1982 and the Criminal Procedure Act 51 of 1977. Under the security laws in particular arbitrary searches could be done and the police also had wide powers of detention. See D J McQuoid-Mason “The right to privacy, honour and reputation” in M Robertson (ed) *Human Rights for South Africa* (1991) at 89.

²⁵⁸ Section 198(c), Act 108 of 1996.

²⁵⁹ Section 199(5), Act 108 of 1996.

²⁶⁰ David Shapshak “SA Services Get Smart” *Mail & Guardian*, April 24, 1998.

to a lot of personal information. Care will have to be taken to regulate and enforce the use of these cards in such a way as not to infringe on privacy rights.

2.2.4 Biometrics

Biometrics is the process of collecting, processing and storing details of a person's physical characteristics for the purpose of identification and authentication.²⁶¹ The most popular forms of biometric identification are retina scans, hand geometry, thumb scans, fingerprints, voice recognition, and digitised (electronically stored) photographs.²⁶² Biometrics schemes are being implemented across the world.²⁶³ Finger print identification is also used in South Africa and in Nigeria. Finger print information is contained on the national driver's license in both countries and for identity documents in South Africa.

Biometric identification is however not as common as the other forms of technology discussed in this chapter, therefore it is only intended to mention the technology briefly. DNA identification is presently a controversial form of biometrics.²⁶⁴ It involves the use

²⁶¹ Banisar op cit at <http://www.gilc.org/privacy/survey/intro.html#defining>.

²⁶² Ibid. See also S Garfinkel *Database Nation: The Death of Privacy in the 21st Century* (2000) at 55-59.

²⁶³ In Germany and France, tests were put in place with equipment that put finger print information on credit cards in 1998. Spain also has a national finger print system for unemployment benefit and healthcare entitlement. Cf Banisar op cit at <http://www.gilc.org/privacy/survey/intro.html#defining>.

²⁶⁴ Cf Garfinkel op cit at 46ff.

of scanning technology, which can automatically match DNA samples against a large database in minutes.²⁶⁵

It is being used by police forces in several countries such as the United States, Germany, and Canada that are creating national databases of DNA.²⁶⁶ This has implications for the right to privacy²⁶⁷ and as such, mention is made of it in view of the fact that this work aims at bridging the gap between technology and the law of privacy, and placing the law ahead of technology.

2.2.5 Surveillance devices

One major way in which the pattern of life has been affected by technological devices is by the use of surveillance devices that specifically enhance eavesdropping and spying.²⁶⁸ Surveillance equipment has been commonly used by both private and government bodies for over four decades.²⁶⁹ Of the kinds of surveillance equipment used today, the Closed Circuit Television Camera is the most ubiquitous. These cameras are very common in developed countries like the United Kingdom and the United States of America.²⁷⁰ They

²⁶⁵ Ibid.

²⁶⁶ Ibid. In *People v Castro* 144 Misc.2d 956, 545 NYS.2d 985 (SCt 1989), where the court accepted the state's DNA evidence, ruling that DNA testing was generally accepted by science. See also *Cobey v State* 80 Md. App 31, 559 A.2d3a1 ((Md) App 1989), where the Maryland State Supreme Court ruled that DNA evidence could be admitted but should not necessarily be admissible in all criminal trials.

²⁶⁷ A stored biometric may be copied. Cf Garfinkel op cit at 65.

²⁶⁸ See generally A F Westin *Privacy and Freedom* (1967) at 69ff.

²⁶⁹ Westin, writing in 1967 said, " Surveillance equipment is readily available and actively promoted for use" op cit at 102.

are also very common in South Africa, especially in shops, malls, supermarkets, banks and other public places.

Closed Circuit Television Cameras are used in every aspect of urban life and is found in residences, schools, car parks, railway stations and petrol stations. They are used to monitor road traffic, the use of public telephones, cash machines, retail and commercial enterprises, shopping malls, and even hospitals and stadiums.²⁷¹ In the United Kingdom, there are internal codes of conduct established by local authorities, police forces and other bodies responsible for managing schemes, which specify how systems should be used. However, these are inadequate as many schemes that border on invasion of privacy are left un-addressed.²⁷²

It has also been noted that few of these codes specify the basis on which tracking should occur, what constitutes suspicious behaviour and the kind of limitation that should be placed on the length of time a camera is trained on a single person or group in the expectation of an incident occurring.²⁷³ In Britain, the Local Government Information Unit has published a model code of conduct in 1996 and existing codes of conduct have been amended to safeguard the privacy of individuals.²⁷⁴

²⁷⁰ C Norris & G Armstrong *The Maximum Surveillance Society* (1999) at 42.

²⁷¹ Norris & Armstrong *op cit* at 42-55.

²⁷² *Ibid* at 100 & 101.

²⁷³ M Bulos & C Sarno *Codes of Practice and Public Closed Circuit Television Systems* (1996) at 24.

²⁷⁴ Bulos & Sarno *op cit* at 101ff.

In South Africa, the Closed-Circuit Television Camera is very common in public places like shopping malls, and generally in the cities as a crime prevention measure. The reality regarding closed circuit television and other surveillance technology however is that, while they are being used as a deterrent for crime, they are also a means of invading privacy and gathering information.

Generally in the United Kingdom and the United States, there appears to be no specific law regulating such questions as who may be watched, for what reasons and for how long, neither does the Common Law or Human Rights Act provide a proper basis for a challenge based on infringements of the right to privacy in a public place.²⁷⁵

In South Africa however, the law recognises the right of a person not to be followed about or stalked in a public place.²⁷⁶ Legal action may be brought where a person has been stalked, watched or followed “unreasonably” and the test of reasonableness will be applied to determine whether in the circumstances, a claim to protection of the plaintiff’s privacy should be upheld.²⁷⁷

²⁷⁵ Norris & Armstrong op cit at 100.

²⁷⁶ *Epstein v Epstein* (1906) TH 87, see Wessels J at 88, *R v Ferreira* (1943) NPD 19 at 21. See generally McQuoid-Mason op cit at 87ff, 154, where he points out that the test to be applied is the test of reasonableness, and that the question is whether the shadowing complained of was reasonable in the circumstances.

²⁷⁷ Cf McQuoid-Mason op cit 154.

In the United States of America, it has been held to be actionable to shadow a person openly and persistently, in a “rough” and “overzealous” manner.²⁷⁸ In Nigeria, although people are watched by law enforcement agents in public places, the use of surveillance cameras is far less common and there is no legislation governing or regulating their use.

It is suggested in this regard that the Constitutional²⁷⁹ provisions guaranteeing the right to dignity,²⁸⁰ right to personal liberty,²⁸¹ and freedom of movement²⁸² should be relied on to regulate such watching, and on the basis of these provisions, where a person has been roughly, openly, over-zealously, or unreasonably followed or watched, so as to cause him or her inconvenience or embarrassment, such conduct should be unconstitutional. It is submitted that, what constitutes “rough”, “open”, “over-zealous” or “unreasonable” following or watching will have to be determined by the courts from the manner, intensity and other factors involved in the “watching”, based on the circumstances of each case.²⁸³

It must be noted that government use of surveillance devices and intrusions into a citizen’s privacy falls into a separate category from private invasions of privacy. In their duty to maintain law and order and protect persons, property, and national security,

²⁷⁸ P Keeton & R E Keeton *Cases and Materials on the Law of Torts* (1977) 2nd ed at 1102; See generally McQuoid-Mason op cit at 155.

²⁷⁹ 1999 Constitution FRN.

²⁸⁰ Section 34.

²⁸¹ Section 35.

²⁸² Section 41.

²⁸³ See also McQuoid-Mason op cit at 154ff.

government law enforcement agencies have a legitimate claim to the use of physical surveillance, within the limits set by law. Police surveillance, for instance, has been practised for decades.²⁸⁴

However, the development of technology in the twentieth century has brought greater effectiveness to the practice of subversive activities and crime and governments have attempted to keep pace with them. Surveillance cameras are located in strategic positions, and other scientific techniques and instruments such as ballistics, fingerprinting, DNA analysis and spectrographic analysis have been adopted to increase the accuracy of investigations.²⁸⁵

Regulations that promote surveillance have been made in a number of countries. In July 2000, the United Kingdom approved the Regulation of Investigatory Powers Act, which requires that Internet Service Providers provide a reasonable interruption capability in their networks (to be forwarded to government).²⁸⁶ In June 2001, the South African Cabinet approved the Interception and Monitoring Bill²⁸⁷ requiring that telephone companies build in surveillance technology.²⁸⁸ Furthermore, the South African

²⁸⁴ Cf Westin op cit at 117 where he observes that “from the early days of police enforcement and investigation, law and public opinion have accepted such police techniques as shadowing, simple eavesdropping, using informers, planting agents in conspiracies.”

²⁸⁵ Cf Westin op cit at 118.

²⁸⁶ D Banisar op cit at <http://www.privacy.org/pi/summary/phr2000/threats.html#fn4>.

²⁸⁷ The Interception and Monitoring Bill [B50-2001] August 2001 (introduced in the National assembly as a Section 75 Bill).

²⁸⁸ Section 7.

Interception and Monitoring Prohibition Amendment Act²⁸⁹ allows for the interception, with a court order, of mobile telephone communications and widespread surveillance for the purpose of protecting national security.²⁹⁰

It is submitted that in spite of the undesirability of the fact that such laws permit a degree of invasion of privacy, it is advantageous to monitor the use of technology to prevent subversive and criminal acts, such as the detonation of bombs.²⁹¹ In this case, and in all other cases involving government use of technological surveillance, it has been said that the two important interests of public safety and individual liberty must be balanced.²⁹² In democratic societies surveillance devices should be used within the ambit of the relevant Constitution and other laws.

2.3 Conclusion

It is clear from the above brief overview that modern technological devices and immense improvements on the older technology (for instance, photography)²⁹³ greatly facilitate invasions of privacy, and that no one is excluded from potential intrusion and disclosure.

²⁸⁹The Interception and Monitoring (Prohibition) Amendment Act 127 of 1992. Cf below Para 7.1.2.1.2 .

²⁹⁰ See generally the Preamble, Sections 3, 6 & 7.

²⁹¹ For instance the London bombings of July 7, 2005.

²⁹² See Westin op cit at 117f.

²⁹³ Although invasions of privacy involving photography have been an issue for over a century, as evidenced in *Pollard v Photographic Co* (1889) 40 Ch.D. 345, they remain relevant in the present day, supra.

Moreover, there is no aspect of life that is completely protected from such unwanted intrusion and disclosure.

Disclosures are made possible by the use of the above technological monitoring and surveillance devices, data processing networks, pools of information and the Internet, which readily provide a convenient and effective means of publication to “the whole world” since there is hardly any limit to the distance that information can travel via the Internet.

In addition to the threats to privacy posed by the use of the Internet,²⁹⁴ computers in Internet cafes may be regarded as depositories or banks of varying amounts of personal information relating to the internet café users.²⁹⁵ As these computers are available for public use, there is a risk that personal information contained in and/or obtained from the computers may be accessed, disclosed or used in some other way by a third party.

The need for adequate legal machinery for the protection of privacy in the face of continuing technological advancements is a pressing issue. It is now intended to examine the protection of the right to privacy generally, as well as data protection in the technologically advanced countries of the United Kingdom, the United States of America and Germany.

²⁹⁴ Cf above Para 1.2ff.

²⁹⁵ Cf above p 21.

CHAPTER THREE

PROTECTION OF PRIVACY AND DATA IN THE UNITED KINGDOM

3.1 Introduction

The right to privacy is expressly guaranteed in a number of international and regional conventions. The Universal Declaration of Human Rights,²⁹⁶ The International Covenant on Civil and Political Rights,²⁹⁷ The European Convention on Human Rights,²⁹⁸ and The American Convention on Human Rights.²⁹⁹ The African Charter on Human and Peoples' Rights does not expressly recognise the right to privacy, but does refer to dignity.³⁰⁰ The provisions of these conventions are applicable to party or signatory nations and the courts are bound to uphold and enforce them whenever they are invoked.³⁰¹

3.2 Protection of Privacy and Data in the United Kingdom

²⁹⁶ Article 12.

²⁹⁷ Article 17.

²⁹⁸ Article 8.

²⁹⁹ Article 11.

³⁰⁰ Article 5.

³⁰¹ See for instance *Klass and Others v Germany* (1978) 2 EHRR 214; where five German lawyers sought to challenge the compatibility with the ECHR of Article 10 (2) of the German Constitution and another Act which provided authority for the German intelligence services to intercept communications; See also *Halford v United Kingdom* (1997) 24 EHRR 523.

Until the coming into effect of the Human Rights Act,³⁰² there was no general right of privacy in the United Kingdom.³⁰³ The United Kingdom does not have a written constitution and the general liberties of its citizens are theoretically protected by Parliament.³⁰⁴ The Common Law protection of privacy and data in the United Kingdom will be examined first, thereafter reference will be made to the Human Rights Act and its effect on the right to privacy in the United Kingdom.

3.2.1 Substantive and Informational Privacy Rights³⁰⁵

Privacy rights have been generally classified as either substantive or informational.

3.2.1a Substantive privacy rights

Substantive privacy rights relate to human beings and their right to personal autonomy.³⁰⁶

They permit individuals to freely act, choose and make their own decisions about matters

³⁰² 1998 Chapter 42, The Act came into effect in Scotland on 1 October 2000, and in England on 1 October 2001.

³⁰³ *Kaye v Robertson* [1991] FSR 62; *Malone v Metropolitan Police Commissioner* [1979] Ch 344, [1979] 2 All ER 620.

³⁰⁴ D Banisar & S Davies "Privacy and Human Rights: An International Survey of Privacy Laws and Practice" (1999) <http://www.gilc.org/privacy/intro.html> at http://www.gilc.org/privacy/survey/survey1z.html#united_kingdom Accessed September 2000.

³⁰⁵ The classification of privacy rights into substantive and informational privacy rights is better recognised in the United States than the United Kingdom. Apposite cases and examples from the United States have thus been used here.

³⁰⁶ See Cf D McQuoid-Mason "Privacy" in M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz, S Woolman (eds) *Constitutional Law of South Africa* (2004) at 38-22 ff.

of a personal nature without interference by the state.³⁰⁷ Such matters include the home, family or personal relationships, marriage, cohabitation, procreation, education, contraception and other such rights of a personal nature.³⁰⁸ Substantive privacy rights are exercisable by persons basically by virtue of the fact of being human. As substantive rights relate to matters of a human nature, it is reasonable that the protection they offer be limited to natural persons only.³⁰⁹

English Common Law has recognized the protection of privacy rights that may be classified as substantive especially in protecting the right not to disclose confidential information in family relationships.³¹⁰

Where the interest of the state necessitates an infringement of a privacy right, such infringement will be justified if that state interest is shown to be of a compelling nature.³¹¹ Further to this, it has been said that it is not sufficient for a statute infringing on the right to privacy to be reasonably related to the carrying out of a permissible state policy.³¹² The infringing statute must be shown to be necessary. In this regard, a law

³⁰⁷ See W P Keeton, D B Dobbs, R E Keeton & D G Owen *Prosser and Keeton on the Law of Torts* (1984) 5th ed at 866. See also 16A *American Jurisprudence 2d Constitutional Law* (1979) Articles 601-606.

³⁰⁸ *Bowers v Hardwick* (1986) 478 US 186, L Ed 2d 140, 146, 106 SCt 2481.

³⁰⁹ 16A *American Jurisprudence 2d Constitutional Law* (1979) 606.

³¹⁰ *Argyll v Argyll* [1965] 1 All ER 611, [1967] Ch 308. Cf below Para 3.2.2.1.1.1.

³¹¹ See du Plessis & J de Ville "Personal Rights" in D Van Wyk, J Dugard, B de Villiers, & D Davis (eds) *Rights and Constitutionalism: The New South African Legal Order* (1994) at 244.

³¹² Goldberg J in *Griswold v Connecticut* supra at 523, See also *Hill v National Collegiate Athletic Association* (1990 6th Dist) 1 Cal App 4th 1398. See generally Van Wyk et al op cit at 243-244.

which gave a restrictive definition of family and then limited the occupancy of any dwelling unit to members of the same family was declared invalid.³¹³ Similarly, a Connecticut statute which criminalized procuring an abortion except for the purpose of saving the life of the mother,³¹⁴ and a state law which criminalized interracial marriage³¹⁵ were considered infringements of substantive privacy rights in the absence of compelling state interests and declared invalid.³¹⁶

3.2.1b Informational Privacy Rights

Unlike substantive privacy rights which relate essentially to human beings and protect their choices, informational privacy rights relate directly to and protect (personal, private or confidential) information by regulating access to and the use of personal information relating to others.³¹⁷ Although it has been held that juristic persons generally do not have a right to privacy,³¹⁸ it has been established that they have a right to claim protection in respect of certain rights analogous to informational privacy rights.³¹⁹

³¹³ *Moore v East Cleveland* (1977) 431 US 494, 52 L Ed 2d 531, 97 SCt 1932.

³¹⁴ *Griswold v Connecticut* supra.

³¹⁵ *Loving v Virginia* (1967) 388 US 1, 18 L Ed 2d 1010, 87 SCt 1817.

³¹⁶ Cf du Plessis & de Ville in Van Wyk et al op cit at 244 ff.

³¹⁷ See generally McQuoid-Mason in Chaskalson et al op cit at 38-25ff.

³¹⁸ 16 *Am Jur 2d Constitutional Law* (1979) Article 606; See also *California Bankers Association v Schultz* (1974) 416 U.S. 21, 65; *U.S. v Morton Salt Co.*, (1950) 338 US 632, 652.

³¹⁹ For instance under the *Restatement (Third) Unfair Competition* (1995) Section 43, confidential business information is treated as property and corporate espionage may be prosecuted as an improper acquisition of a trade secret. Similarly, under trademark laws, a business can own a product name and prevent others from using the same product name. Under the category of appropriation, where a business name or product name has been appropriated, a juristic person can successfully bring an action for “invasion of its privacy”. Cf

Informational privacy rights provide protection against intrusions and unauthorised disclosure or publication of personal information relating to others.³²⁰ The United States Privacy Act of 1974³²¹ and the United Kingdom Data Protection Act³²² both provide extensive protection for informational privacy in the form of data. English Common Law also upholds the right not to disclose confidential business information and punishes unauthorised disclosure of the same and as such, recognises informational privacy rights.³²³

Privacy of communication is generally guaranteed under informational privacy rights,³²⁴ and cases of invasion of electronic mail privacy in Internet cafes will fall into this general category. Informational privacy rights will be relevant in Internet cafes in upholding customers' right to privacy in respect of any information processed on computers in Internet cafes by regulating access to and the publication or disclosure of such information.

In *United States v Little*³²⁵ the practice of asking census questions concerning personal and family characteristics and threatening a refusal to reply with criminal sanctions was

also the English cases of *Technograph Printed Circuits Ltd v Chahoy* [1967] RPC 399 at 344 and *Exchange Telegraph Co v Howard* [1906] 22 TLR 375 (Cf below at 82ff).

³²⁰ Cf Roos op cit at 41.

³²¹ (1974) 5 USC Section 552a.

³²² Cap 29 of 1998.

³²³ Cf below Para 3.2.2.1.1.2.

³²⁴ See du Plessis & de Ville in van Wyk et al op cit at 244.

³²⁵ (1971) 321F Supp 388 D Del; See also *United States v Miller* supra.

upheld. This was because the answers could only be used statistically and would never be disclosed so as to identify any individual.

As in the case of substantive privacy rights, when weighing the right to privacy against other interests, public interest may override informational privacy rights. In *Nixon v Administrator of General Services*,³²⁶ the Supreme Court established that although the President had an interest in the informational privacy of his official records, his interest was outweighed by the public interest in those records.

3.2. 2 Common Law Protection of Privacy and Data in the United Kingdom

3.2.2.I Common Law Protection of Privacy

In the 19th century, an English writer had observed:

“The laws of the land are intended not only to preserve the person and material property of every citizen sacred from intrusion, but to secure the privacy of his thoughts, so far as he sees fit to withhold them from others. Silence is as great a privilege as speech, and it is as important that everyone should be able to maintain it whenever he pleases, as that he should be at liberty to utter his thoughts without restraint.”³²⁷

³²⁶ (1970) 433 US 425.

³²⁷ J Holbrook *Ten Years Among the Mail Bags* (1855) at xviii.

This suggests that there was an awareness of the need for individual or personal privacy during the 19th Century, even though the Common Law did not recognise a specific right to privacy. However, notwithstanding the absence of a Common Law right to privacy, an infringement of privacy could be actionable at Common Law, if the plaintiff could bring his or her complaint within one of the existing nominate torts, or in equity, under the rules of confidentiality for breach of confidence.³²⁸

Under the rules of 'Equity', one who receives information under express (or implied) conditions of confidence³²⁹ is under a duty not to reveal it.³³⁰ Thus private and personal confidences were protected by the law relating to breach of confidence based on misuse of information.

Under the rules of Equity, an action may also be brought for breach of commercial confidence where a person uses another's confidential material for his own commercial gain.³³¹ This equitable remedy protects confidential information in general including business interests, and information which a company or business generates about its own activities.³³²

³²⁸ See generally *McQuoid-Mason* op cit at 49ff.

³²⁹ *Saltman Engineering v Campbell Engineering* [1948] 65 RPC 203; *Terrapin v Builders' Supply Co (Hayes) Ltd* [1967] RPC 375.

³³⁰ See Lord Goff of Chieveley in *Attorney General v Guardian Newspapers (No 2)* [1990] 1 AC 109 at 281; See also H Pearson & C Miller *Commercial Exploitation of Intellectual Property* (1990) at 30-31.

³³¹ *Morison v Moat* [1851] 9 Hare 241, *Saltman Engineering v Campbell Engineering* supra; See also *McQuoid-Mason* op cit at 53.

In *Thomas Marshall (Exporters) Ltd v Guinle*³³³ such information as the names and telex addresses of the company's manufacturers and suppliers and their individual contacts; details of the company's current negotiations; information as to the requirements of the company's customers; the company's new ranges actual or proposed; the company's samples and negotiated prices paid to the company by customers were held to be capable of being confidential.³³⁴

A duty of confidence has also been held to arise out of a professional relationship.³³⁵ The law imposes an obligation to maintain the confidentiality of disclosures made to certain persons in their professional capacity. Such professionals include lawyers³³⁶, medical practitioners,³³⁷ and bankers.³³⁸ It has been held at Common Law that a prisoner has the right to communicate with his or her lawyer with almost no interference.³³⁹

³³² See generally F Gurry *Breach of Confidence* (1984) at 92ff.

³³³ [1978] 3 WLR 116.

³³⁴ Per Megarry V.C. at 136.

³³⁵ *Prince Jefri Bolkiah v KPMG* [1999] 1 All ER 577. See generally Gurry op cit at 143ff.

³³⁶ In *Lord Ashburton v Pape* [1913] 2 Ch 469, it was established that a solicitor has a duty of confidentiality in respect of any information received directly from a client, such as letters. See generally *Minter v Priest* [1930] AC 558.

³³⁷ In *Hunter v Mann* [1974] 1 QB 767, the duty of a doctor not to disclose [voluntarily] information obtained in his professional capacity without the consent of his patient was affirmed. See also *AB v CD* (1851) 14 Dunlop 177.

³³⁸ In *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461, it was held that it was an implied term in the banker's contract with the customer that the banker shall not disclose the account, or transactions relating thereto, of his customer except in certain circumstances. Per Scrutton J at 480.

³³⁹ *Golder v United Kingdom* (1975) 1 EHRR 524; See generally *Minter v Priest* supra at 581ff.

Where a person employs improper methods to obtain information that the owner has not made public, or consented to the publication of, action may also be brought to protect the form in which the ideas are expressed for breach of copyright.³⁴⁰ Under the Common Law, personal confidences were also protected by the law of contract, where there was an express stipulation as to confidentiality in the agreement of the parties, the plaintiff could sue for a breach of contract.³⁴¹ There is however no liability on the part of defendant for breach of contract where no contract exists.³⁴²

In classifying the cases where the right to privacy has been protected by the Common Law courts, two broad categories have emerged. The first category consists of cases where a broad duty of good faith exists and is breached.³⁴³ In the other category, the litigant fits the invasion of privacy into one of the traditional areas of tort and the courts give a remedy based on the breach of duty protected by that tort. Here, the courts have usually classified the information revealed as property and protected the property rights of the plaintiff.³⁴⁴ However, the law of privacy, as it stands at Common Law today appears to have evolved from cases relating to confidential information.³⁴⁵

³⁴⁰ *Millar v Taylor* [1769] 98 ER 201.

³⁴¹ *Thomas Marshall (Exports) v Guinle* supra where the defendant was employed under a contract of employment which forbade disclosure of confidential information while employed, and disclosure or use afterwards; See also *Robb v Green* [1895] 2 QB 1 where confidentiality was emphasised in the defendant's interview for the job; Cf *Morison v Moat* (1851] 9 Hare 241.

³⁴² In *Sports & General Press Agency Ltd v "Our Dogs" Publishing Co* (1917) 2 KB 125 (CA), it was held that a photographer may sell photographs taken at a dog show if there is no restriction on the taking of such photographs.

³⁴³ See *Argyll v Argyll* supra; See also Lord Denning in *Seager v Copydex* [1967] RPC 349 at 368; [1967] 1 WLR 923 at 931. (Cf below).

3.2.2.1.1 Breach of Confidence

The Common Law action of breach of confidence is founded on Equity.³⁴⁶ For an action in breach of confidence to succeed, three criteria must be satisfied:

(a) The information allegedly protected by the obligation of confidence must be legal and of a kind which the law will protect.³⁴⁷

(b) The information must have been obtained by some party other than the “owner” of the information in circumstances under which a duty of good faith will be imposed.³⁴⁸

(c) The other party must have acted, or be about to act in a manner not compatible with a duty of good faith, or in a manner which was a breach of some other duty, (i.e. there must be an actual or imminent breach of good faith or other legal duty).³⁴⁹

In *Attorney General v Guardian Newspapers Ltd. (No 2)*,³⁵⁰ Lord Goff of Chieveley laid down the conditions under which a duty of confidence would be held to exist as follows:

³⁴⁴ See *Herbert Morris Ltd v Saxelby* [1916] 1 AC 688 at 714; *Technograph Printed Circuits Ltd v Chahoy* supra at 344.

³⁴⁵ Lord Denning, apparently referring to *Albert v Strange* [1849] 2 De G & Sm 652, 64 ER 293 (Ch) during the debate on Lord Mancroft’s Right of Privacy Bill: “So in 1848, the courts of this country were ready to give a remedy for the infringement of privacy.” *House of Lords’ Debates* (1961) Vol 229, Col 638. Cf *McQuoid-Mason* op cit at 49ff. See also S D Warren and L D Brandeis “The Right to Privacy” (1890) 4 *Harvard Law Review* 194 at 202ff.

³⁴⁶ Cf Lord Denning in *Seager v Copydex* supra at 931: “The law on this subject ... depends on the broad principle of equity that he who has received information in confidence shall not take unfair advantage of it.”

³⁴⁷ See for instance *Khasoggi v Smith* [1980] 130 NLJ 168 (CA).

³⁴⁸ *Seager v Copydex* supra; *Terrapin Ltd v Builders’ Supply Co (Hayes) Ltd* supra.

³⁴⁹ J Phillips & A Firth *Introduction to Intellectual Property Law* (1995) 229ff.

³⁵⁰ *Supra*.

“A duty of confidence arises when confidential information comes to the knowledge of a person in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.”³⁵¹

It has also been suggested that a duty of confidence will be imposed in situations where a person innocently acquires information that is obviously confidential, even though there is no fiduciary relationship between them.³⁵² In *Francome v Mirror Group Newspapers Ltd*,³⁵³ where the defendant eavesdropped on telephone conversations by means of a radio-telephone device under circumstances where the plaintiffs obviously intended their conversation to be private, the court held that the defendant was under a duty not to disclose the information so obtained. It appears that the courts are more likely to impose liability, or, a duty of confidence, where information is acquired by improper or unlawful means.³⁵⁴

³⁵¹ At 281.

³⁵² *Ibid.* In *X Ltd v Morgan Grampian (Publishers) Ltd* [1991] 1 AC 1, it was suggested that a thief who steals a document, which is obviously confidential may be impressed with a duty of confidence. *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, where it was suggested that a photographer with a long-range photo lens would owe a duty of confidentiality to a subject who was engaged in a private act and not expecting to be photographed. (Per Laws J at 807). See also *Barrymore v News Group Newspapers Ltd* [1997] FSR 600, *Stephens v Avery* [1988] 1 Ch 449.

³⁵³ [1984] 1 WLR 892.

³⁵⁴ In *Douglas v Hello! Ltd* [2001] QB 967; [2002] 1 FCR 289; [2003] EWHC 786, where the defendants unlawfully took pictures of the plaintiffs, in awarding judgement for the plaintiff, the court took into account the fact that the taking of the photographs by the defendants must have involved a trespass. See also *Shelley Films v Rex Features* [1994] EMLR 134.

3.2.2.1.1 (a) Relevance to Internet Cafes

Although the sending of e-mail in Internet cafes has only become popular within the last six years, and is probably practiced more in Nigeria than in the United Kingdom,³⁵⁵ English Common Law contains cases of misuse of information tantamount to invasions of privacy. Some of the principles applied by the courts in these cases may provide guidance for the protection of privacy and data in Internet cafes in Nigeria.

The English law of confidentiality does offer valuable principles, applicable to the protection of e-mail in Internet cafes. It is trite, and Internet café owners ought to be aware, that information sent and received in Internet cafes may be personal, and of a confidential nature. On this basis, it is submitted that, following the English Common Law, a fiduciary relationship ought to be implied between an Internet café owner and his or her clients with regard to information processed in Internet cafes, and a corresponding duty of confidence should be imposed on Internet café owners and their staff concerning information processed by customers in their Internet cafes.

In this regard, it is submitted that where an Internet café owner accesses, publishes or otherwise uses personal information relating to a client by unlawful means and, or, without lawful authorisation or justification, the Internet café owner will be in breach of the duty of confidence owed to that client.

³⁵⁵ The United Kingdom is a developed economy as opposed to Nigeria therefore computer, e-mail and Internet facilities are likely to be more accessible to the individual for instance, at home, at work, in public

It may be argued that given the nature of Internet cafes, Internet café users ought to be aware of the threat to their privacy posed by the sharing of computers in Internet cafes and the additional risk of Internet café staff coming into contact with personal information, and as such, the principle of *volenti non fit injuria* should be applied generally to Internet-café related cases of invasions of privacy.

However, it is submitted that the proper position should be that Internet café customers will be deemed to give their consent and authorisation to Internet café staff for access to personal information:

- (a) where the staff come into contact with such information in the ordinary course of duty or,
- (b) where download is necessary strictly for purposes and under conditions clearly set out and made known to the customer prior to such download for the direct benefit of, or, in the interest of customers and, or, for the effective running of the facility.

In this regard, it is recommended as an effectual measure towards providing Internet café privacy that Internet café owners be required to clearly and unequivocally set out the activities as well as conditions which in the course of their duty usually require or involve access to and the downloading of information relating to customers. This list of conditions should be made available to every first-time customer in the form of a printed document or as the first page on any Internet cafe computer, together with a requirement

libraries and in academic institutions, than in Nigeria. As such, there will be far less need for Internet cafes in the United Kingdom than there is in Nigeria.

that customers should read and signify their consent to these conditions in order to proceed with their use of the computer(s).

The conditions set out by Internet café owners will outline the boundaries for access to and use of personal information relating to customers by Internet café staff and, or, owner(s). Any use by staff (or owner/s) of personal information relating to customers falling outside of these specified perimeters will *prima facie* constitute an invasion of customers' privacy for which Internet café staff and, or, owner(s) will be liable, unless proved otherwise.

We shall proceed to examine English law breach of confidentiality cases in greater detail for a more in-depth analysis of the courts' construction and application of the principle.

For present purposes, we shall classify breach of confidentiality cases into two broad categories:

- (a) Invasions into personal and family matters
- (b) Invasions into business matters.³⁵⁶

Bearing in mind that a specific right to privacy was not recognised in any of the following cases, instances of invasions into personal and family matters will, for our purpose represent cases upholding substantive privacy rights, while cases on invasions

³⁵⁶ For present and further purposes in this work, "business matters" will include invasions not strictly domestic, or family related (e.g. invasions into civic and political life, the affairs of customers, invasions relating to professional, business or educational institutions e.t.c.).

into business matters will be used as examples of instances where informational privacy rights have been upheld.

We shall now examine cases on breach of confidentiality concerning family matters.

3.2.2.1.1 Breach of Confidence Concerning Family Matters

In *Argyll v Argyll*,³⁵⁷ an injunction was granted based on marital confidence to restrain publication of letters containing secrets and confidences exchanged between the Duke and Duchess of Argyll during their marriage. The court was of the opinion that the mutual trust and confidences shared between husband and wife within the relationship of marriage were intimate and confidential.³⁵⁸

However, in *Lennon v News Group Newspapers and Twist*,³⁵⁹ the application of the plaintiff to restrain a newsgroup from publishing an article by his ex-wife was refused. In this case, Lord Denning was of the opinion that the relationship of the parties had “ceased to be their own private affair” as it had been put into the “public domain.”³⁶⁰

The courts have also actively upheld the public interest in allowing the exposure of a wrong.³⁶¹ In *Mrs R v Central Television PLC*³⁶² a photograph was obtained on private

³⁵⁷ *Supra*.

³⁵⁸ Per Ungood Thomas J at 619.

³⁵⁹ [1978] FSR 573 (HL).

³⁶⁰ At 574-5.

³⁶¹ In *Gartside v Outram* [1857] 26 LJNS Ch 113, Wood V.C. said: “The true principle is that there is no confidence as to the disclosure of iniquity.” See also *Lion Laboratories v Evans* [1985] 1 QB 526; [1984] 3 WLR 539. In this case, information about the doubtfulness of the accuracy of the Lion Intoximeter breath-

property without the consent of the owner in circumstances where the publication might have been thought to seriously prejudice the welfare of a child. The court upheld the publication of the photographs in the interest of freedom of speech.

In English law, it appears that where a newspaper or news agency publishes details of a person's private life, an action based on breach of confidence, will ordinarily, not succeed.³⁶³ In *Woodward v Hutchins*,³⁶⁴ the plaintiffs, who were pop stars applied for an injunction restraining publication of articles revealing information about their behaviour and private lives. The court held that since the plaintiffs had sought publicity in respect of their private lives, they could not complain about the truth being publicised about them.

³⁶⁵ The injunction was refused.

In *A v B Plc*³⁶⁶ where the claimant, sought an injunction to prevent the publication of information about his extra-marital affairs, the court of first instance granted the claimant an injunction on the grounds that the law of confidence should protect sexual

testing apparatus was revealed to the press by a former employee of the company. The public interest defence succeeded. The court, in this case, distinguished between matters of public interest and matters of interest to the public (at 537). Similarly in *Initial Services v Putterhill* [1968] 1 QB 396, a former employee of the company revealed information about alleged illegal price fixing concerning the company. The public interest defence succeeded. Although the *Lion Laboratories* and the *Initial Services* cases were business-related cases, the reasoning of the court in allowing the disclosure of confidential information is relevant.

³⁶² [1994] *Fam* 192.

³⁶³ Cf R Wacks *The Protection of Privacy* (1980) at 84.

³⁶⁴ [1977] 2 All ER 751; [1977] 1 WLR 760. See also *Khasoggi v Smith* supra where the plaintiff, a wealthy woman and public figure sought an injunction to restrain her former housekeeper and a newspaper from disclosing confidential information involving allegations of criminal misconduct and sexual affairs. The injunction was refused.

³⁶⁵ See Bridge LJ "...those who seek and welcome publicity ... so long as it shows them in a favourable light are in no position to complain of an invasion of their privacy by publicity which shows them in an unfavourable light." [1977] 1 WLR 760 at 765; See also Lord Denning (MR) at 763-4.

³⁶⁶ [2001] 1 WLR 2341.

relationships within and outside marriage,³⁶⁷ and that there was no public interest in the publication of the information.

On appeal, a distinction was made between the status accorded by law to a marital relationship on the one hand, and the nature of the relationship that the claimant had on the other hand. The court was reluctant to enforce or protect a right to privacy when there was public interest in exposing a wrong or, where the information, which was the subject of the protection was already public knowledge or to uphold the right to freedom of speech.³⁶⁸ The defendants' appeal was allowed on the basis that they had lawfully exercised the right to freedom of the press.

Generally, it appears to be an acceptable principle, which has also been upheld by the English courts, that people who are considered to be "public figures" give-up a degree of the privacy to which they might otherwise have been entitled.³⁶⁹ However, it has been contended that the fact that the plaintiff has "courted publicity" should not be a reason to deny him or her redress for breach of confidence since the action is based on the equitable principle that the defendant should not take unfair advantage of the plaintiff's confidence.³⁷⁰

³⁶⁷ Per Jack J at 2354.

³⁶⁸ [2003] QB 195.

³⁶⁹ Warren & Brandeis op cit at 215-6, Prosser at 823-830. In *New York Times v Sullivan*, (1964) 376 US 254, the Supreme Court held that a public figure is entitled to less protection by the law of defamation than a private person. Cf *McQuoid-mason* op cit at 219ff.

³⁷⁰ Wacks op cit at 85.

3.2.2.1.1.1 (a) Relevance to Internet Cafes

In English law it is clear that information relating to marital relationships will be protected under the law of confidentiality and it is suggested that marital information should be so protected when processed in Internet cafes in Nigeria. However it appears that the English Common Law has been reluctant to extend the same protection to information relating to extra-marital relationships.³⁷¹

Nonetheless, it is suggested for Nigerian purposes that, a duty of confidence should *prima facie* be extended to all information (including information concerning extra-marital relationships) processed in Internet cafes in Nigeria.

Given the relative ease of access to, and widespread publication achievable through, the Internet, the potential for irreparable damage to privacy (as well as reputation) is far greater today. It is thus suggested that to ensure effective protection, the focus of data and privacy protection laws should be the prevention of unlawful disclosure rather than the award of damages or redress after the fact. Furthermore, the denial of legal protection for information relating to extra-marital relationships may, unintended by the law, give a license for unreasonable intrusions, sensational news scavenging and the spread of gossip, which, though of interest to the public, must be distinguished from publication in the public interest.³⁷²

³⁷¹ *A v B Plc* supra; Cf above Para 3.2.2.1.1.1.

³⁷² Cf *Lion Laboratories v Evans* supra; above at Para 3.2.2.1.1.1.

However, in line with the English Common Law position, it is agreed that no one should be bound to conceal illegality.³⁷³ Thus it is suggested that disclosure of information processed in Internet cafes in Nigeria should be permissible and justified where such disclosure is made to law authorities in the performance of their duty or for the service of other legal ends.

Thus where, for example, information concerning smuggling or any other unlawful activity is processed in an Internet cafe, while there will be justification for disclosure of such information to relevant law enforcement agents, there may be liability for disclosure to other Internet café users.

As in the case of extra-marital relationships, it appears that English Common Law protection of the privacy of public figures is narrow. This may however change³⁷⁴ with the adoption of the Human Rights Act.³⁷⁵

With regard to the protection of information processed in Internet cafes in Nigeria, it must first be noted that, knowing the challenge that they face to keep their affairs private and given the semi-public nature of Internet cafés, it is unlikely that information relating to public figures will be processed in Internet cafes by them or their agents. However, given the fact that Nigeria is a developing nation where infrastructure including

³⁷³ Cf Wood V.C. in *Gartside v Outram* supra; see above Para 3.2.2.1.1.1.

³⁷⁴ Cf *Douglas v Hello! Ltd* supra.

³⁷⁵ Chapter 42 of 1998.

communication devices may not always be reliable or sufficiently stable, the use of Internet cafes by public figures might occasionally become necessary.

In such cases, it is suggested that (in line with the general duty of confidence imposed on Internet café owners and staff)³⁷⁶ a duty of confidence should be implied between the Internet café owner and staff on the one hand, and the customer who processed the information on the other hand (whether it be the public figure him/herself or an agent), especially where the plaintiff has taken any steps indicating that he/she intends to keep the information private.

Thus Internet café owners and their staff will be liable where they publish or disclose information relating to public figures processed in their Internet cafes. It is further suggested that in such cases, as in *Albert v Strange*,³⁷⁷ even where they did not process such information in the Internet café by themselves, the public figure concerned should be able to successfully bring action against the Internet café owner and or staff in respect of a threatened or actual unlawful disclosure or publication.

The principle stated by Wacks³⁷⁸ is applicable here, namely that Internet café owner and or staff should not be allowed to take unfair advantage of their customers' confidence, and there should be no exceptions with regard to public figures.³⁷⁹

³⁷⁶ Cf above Para 3.2.2.1.1(a).

³⁷⁷ [1849] 2 De G & Sm 652, 64 Eng Rep 293 (Ch); Cf below Para 3.2.2.1.1.2.

³⁷⁸ Cf above Para 3.2.2.1.1.1.

As for cases of publication by the press, it must first be asserted that public interest may validly override a claim to privacy in respect of unauthorized disclosure or publication of information processed in an internet café. However, here again, it is reaffirmed that there should be a clear distinction between matters of public interest on the one hand and matters of interest to the public on the other hand.³⁸⁰

In this regard it is submitted that the mere fact that publication or disclosure would interest, or be entertaining to the public is not sufficient reason to deny a claim for confidentiality; publication must be positively beneficial to the public, and the denial of a claim to privacy must achieve more good than the satisfaction of the public's insatiable appetite for sensational news.³⁸¹

3.2.2.1.1.2 Breach of Confidence Concerning Business Matters

In *Albert v Strange*,³⁸² etchings made by Prince Albert for private use that had been sent for printing were surreptitiously copied by one of the printer's workmen. When they were subsequently about to be put on public exhibition the defendant printed a catalogue of the works. An injunction was issued by the Lord Chancellor, restraining the defendant from doing so.

³⁷⁹ Ibid.

³⁸⁰ See *Lion Laboratories v Evans* supra at 537; Cf above Para 3.2.2.1.1.1.

³⁸¹ Cf above Para 3.2.2.1.1.1.

³⁸² Supra.

The decision was based on the use of the plaintiff's property in the etchings as well as breach of trust.³⁸³ In this case, an action for breach of confidentiality was successfully brought against a third party with whom the original 'owner' of the confidential information had no direct connection.

In *Morison v Moat*,³⁸⁴ the defendant passed on confidential information between the plaintiff and himself regarding the formula for making a medicine. The plaintiff succeeded in obtaining an injunction restraining the defendant from selling his medicine and from using his secret. In English law, there are many cases dealing with confidential information, particularly trade secrets, where such information is classified as property.³⁸⁵

In *Exchange Telegraph Co v Howard*,³⁸⁶ the Court granted injunctions to restrain the surreptitious obtaining of information by the plaintiff, and also to restrain the plaintiff from disseminating such information, based on the defendants' right of property in confidential information.

In *Herbert Morris Ltd v Saxelby*,³⁸⁷ Lord Shaw of Dumferline remarked that "trade secrets ... may not be taken away by a servant, they are his master's 'property'."

³⁸³ Per Lord Cottenham LC at 40.

³⁸⁴ *Supra*; See also *Robb v Green* [1895] 2 QB 315.

³⁸⁵ Cf Gurry *op cit* at 25, where he observes that the jurisdictional basis of an action for breach of confidence is a mixture of contract, equity and property.

³⁸⁶ *Supra*.

³⁸⁷ *Supra* at 714.

Similarly in *Rolls Royce Ltd v Jeffrey*,³⁸⁸ Lord Radcliffe saw no objection to treating “know-how” as a corporate “asset”, distinct from the physical records in which it was contained. In *Technograph Printed Circuits Ltd v Chahoyan*,³⁸⁹ Plowman J classified the plaintiff’s “proprietary interests” as confidential information, which they were entitled to have protected.

As to the question of whether the protection of confidential information under Common Law should be extended to artificial persons or was limited to natural persons, it appears, from the above cases relating to trade secrets, that the Common Law protected property rights. Thus the information given under circumstances where a duty of confidence exists would be held as confidential irrespective of whether the plaintiff was a natural or an artificial person.³⁹⁰ In addition, under the law of contract, the Common Law courts have upheld conditions stipulating confidentiality in a contract whether the plaintiff was a natural person or juristic person.³⁹¹

3.2.2.1.1.2 (a) Relevance to Internet Cafes

From the cases, it may be asserted that English law provides ample protection for confidential information relating to business, especially as it allows artificial persons as

³⁸⁸ [1962] 1 All ER 801 at 805.

³⁸⁹ *Supra* at 344.

³⁹⁰ See also *Terrapin v Builders’ Supply Co* *supra*, *Seager v Copydex* *supra*, *Saltman Engineering v Campbell Engineering*, *supra*, where the courts implied a duty of confidence in commercial relationships involving companies.

³⁹¹ See *Thomas Marshall (Exports) v Guinle* *supra*. See also *Morison v Moat* *supra*.

well as plaintiffs, who may not in the circumstances have a direct business link with the defendant, to successfully bring action. It is suggested that the same broad measure of protection should be adopted for the protection of business- related information processed in Internet cafes in Nigeria.

Although it may not be accurate to adopt the courts' reasoning in classifying information as property,³⁹² it is argued that in the absence of any clause excluding artificial persons, the general duty of confidence that Internet café owners and staff should owe to clients in respect of information processed in their Internet cafes³⁹³ is sufficient to cover both natural and artificial persons. Thus artificial persons should be able to successfully bring action for breach of confidence concerning information processed in Internet cafes.

As for cases where information relating to a person is processed in an Internet café by another resulting in a threat, or actual case, of misuse of that information by the Internet café owner or staff, it is suggested that, following *Albert v Strange*³⁹⁴ the person to whom the information relates should be able to successfully bring action against the Internet café owner or staff for breach of confidence in respect of the unauthorized use or disclosure of the information.

3.2.2.1.1.3 Conclusion on the Utility of the English Law of Confidentiality for the Protection of Privacy in Internet Cafes

³⁹² Cf below Para 3.2.2.1.2.1.

³⁹³ Cf above Para 3.2.2.1.1(a).

It is submitted that generally, English law breach of confidence cases and some of the principles laid down in them provide functional guidelines for the protection of privacy in Internet cafés in Nigeria. Relying on breach of confidentiality, an Internet café user may prevent or have recourse against wrongful intrusion,³⁹⁵ disclosure or publication,³⁹⁶ and other unlawful use³⁹⁷ of personal³⁹⁸ or business information,³⁹⁹ by an Internet café owner or staff, thus exercising privacy protection rights.⁴⁰⁰

The protection afforded will cover information relating to family and business relationships, and extend to artificial persons. An extension of the traditional breach of confidence laws will also permit certain categories of plaintiffs who were denied protection under the English breach of confidence laws to successfully bring action in similar Internet café cases in Nigeria.⁴⁰¹ Overall it is submitted that English breach of confidence laws provide a good basis for the recognition and provision of privacy protection in Internet cafes in Nigeria.

³⁹⁴ Supra. Cf above Para 3.2.2.1.1.2.

³⁹⁵ Cf *Exchange Telegraph Co v Howard* supra.

³⁹⁶ Cf *Albert v Strange* supra, *Morison v Moat* supra.

³⁹⁷ For instance, publication that could place the plaintiff in a false light.

³⁹⁸ Cf *Albert v Strange* supra.

³⁹⁹ Cf *Morison v Moat* supra, *Rolls Royce Ltd v Jeffrey* supra.

⁴⁰⁰ Cf above Para 1.1.

⁴⁰¹ For example, public figures and plaintiffs in cases of press publication. Cf above Para 3.2.2.1.1.1.

3.2.2.1.2 Common Law Torts Involving Family and Business Matters

The following is a list of torts under which the right to privacy has been recognised under English Common Law.

3.2.2.1.2.1 Trespass

Where there is “direct and immediate”⁴⁰² physical contact or interference with the plaintiff’s person, property, or land, in violating a person’s rights, or a threat of imminent harm to the plaintiff, an action may be brought under this head. In *Sheen v Clegg*⁴⁰³ where the defendant secretly installed a microphone over the plaintiffs’ marital bed, the court awarded damages for trespass against the defendant. The tort of trespass has three categories: trespass to person, trespass to chattel (goods), and trespass to land.⁴⁰⁴

Traditionally, Common Law recognised the following three causes of action as categories of trespass to person: assault, battery and false imprisonment.⁴⁰⁵ In *McCarey v Associated Newspapers (No 2)*,⁴⁰⁶ damages were recovered for loss of reputation as a result of false imprisonment.

⁴⁰² R F V Heuston and R A Buckley (eds) *Salmond & Heuston on the Law of Torts* (1992) at 6.

⁴⁰³ *Daily Telegraph* June 22, 1961.

⁴⁰⁴ Heuston & Buckley op cit at 5.

⁴⁰⁵ M Lunney and K Oliphant *Tort Law Text and Materials* (2003) at 29.

⁴⁰⁶ [1965] 2 QB 86.

Trespass to land consists of entering, remaining, or placing or projecting any object on land in possession of the plaintiff.⁴⁰⁷ However, in the case of trespass to land, if the intrusion takes place without direct contact with the plaintiff's property, and from off the person's land, the action will fail. In *Bernstein [of Leigh (Baron)] v Skyways & General Ltd*,⁴⁰⁸ the plaintiff's property was photographed from an aircraft by the defendants, the plaintiff's claim for trespass failed because his right to use and enjoy his property had not been infringed.

However, in *Anchor Brewhouse Developments v Berkley House (Docklands Developments) Ltd*,⁴⁰⁹ the plaintiff was granted an injunction to restrain the defendants from further over-sailing the plaintiff's property by crane booms. The defendants' act was regarded as an "invasion of airspace".

In the *Anchor Brewhouse* case, the defendants had erected tower cranes on their own land with the booms of the cranes swinging over the plaintiff's land, thereby taking into the defendant's possession airspace to which his neighbour (the plaintiff) was entitled, whereas in *Bernstein's* case, the airplane did not make direct contact with any structure on land.

⁴⁰⁷ See Heuston & Buckley op cit at 44.

⁴⁰⁸ [1978] QB 479.

⁴⁰⁹ [1987] 38 *Building Law Review* 82.

Generally, the tort of trespass protects possession and not ownership.⁴¹⁰ However, in certain cases, where the plaintiff is not in exclusive possession of the property, the action will not succeed.⁴¹¹

Where the invasion of a person's privacy involves interference with his or her person, or property or land in his or her possession, redress may be obtained at Common Law by bringing an action for trespass. Many Common Law cases of interference with property that may now be classified as invasion of privacy have been decided on grounds of trespass to property⁴¹² (or breach of confidence).⁴¹³ It must be noted in this regard that, although the courts have classified information as property in some cases, the characterization of information as property is not universal and has been variously criticised and rejected.⁴¹⁴

⁴¹⁰ *Thompson v Ward* [1953] 2 QB 153 at 158-159, *Attersoll v Stevens* [1808] 1 Taunt. 183, 190. See generally Heuston & Buckley op cit at 51.

⁴¹¹ For instance, a lodger or boarder at a house or in a hotel, a guest at a house, or a patient in a hospital. *Allan v Liverpool Overseers* [1874] LR 9 QB 180 at 191-192. In *Kaye v Robertson* supra where the plaintiff was a patient in a hospital, his action for trespass failed. See generally Heuston & Buckley op cit at 51. See also R Wacks *Privacy and Press Freedom* (1995) at 129, McQuoid-Mason op cit at 50.

⁴¹² See *Herbert Morris Ltd v Saxelby* supra (above at 53), *Technograph Printed Circuits Ltd v Chahoy* supra (above at 53). In *Albert v Strange* (supra), the decision was based on grounds of breach of confidence as well as the plaintiff's property in the etchings.

⁴¹³ *Argyll v Argyll* supra, *Morison v Moat* supra. See above Paras 3.2.2.1.1.1 & 3.2.2.1.1.2.

⁴¹⁴ Latham C.J. in *Federal Commission of Taxation v United Aircraft Corporation* [1943-1944] 68 CLR 525: "Knowledge is valuable, but knowledge is neither real nor personal property..." See also Lord Upjohn in *Boardman v Phipps* [1967] 2 AC 46 at 127ff, dissenting from the notion that information was property said: "... it is not property in any normal sense but equity will restrain its transmission to another if in breach of a confidential relationship." Both jurists adhere strictly to the traditional classification of the action of breach of confidence under the laid down rules of equity. See also Stuckey "The Equitable Action for Breach of Confidence: Is Information Ever Property?" [1981] 9 *Sydney Law Review* 402 at 404.

The more accurate view appears to be that the cases in which information has been treated as property do not necessarily establish a general classification of information as property.⁴¹⁵ It is suggested that information has been characterised as property to protect the interests of the plaintiff in cases where the courts are of the opinion that the plaintiff has a valid claim, but such claim does not fall strictly under any of the nominate torts.⁴¹⁶ In South Africa, the Constitutional Courts regard the right to privacy as an aspect of the right to dignity,⁴¹⁷ instead of property.⁴¹⁸

3.2.2.1.2.1a Relevance to Internet Cafes

The tort of trespass will be useful for the protection of Internet café privacy where the defendant enters the internet café unlawfully or, where the tortfeasor enters lawfully in order to do an unlawful act. Here, the tortfeasor may be liable for trespass *ab initio*.⁴¹⁹ Action may also be brought for trespass to property where invasion of privacy involves the unlawful touching of computers, floppy discs, flash drives or any other storage device in order to access or use information.

⁴¹⁵ N Palmer *Confidentiality and the Law* [1990] at 89.

⁴¹⁶ Cf Palmer *op cit* at 89, where he describes the cases as “*suis generis*”, and, is of the opinion that a proprietary analysis was adopted in those cases as a convenient legal method of reaching a conclusion which may now be achieved without such analysis.

⁴¹⁷ See *National Coalition for Gay and Lesbian Equality & Others v Minister of Justice & Others* 1998 (6) BCLR 726 (W) at Para 30.

⁴¹⁸ See above at 3 & 4. See also J Neethling, J M Potgieter, P J Visser *Law of Delict* (2006) at 352 ff, where the right to dignity is discussed.

⁴¹⁹ Cf G Kodilinye *The Nigerian Law of Torts* (1982) at 177ff.

However, since the tort of trespass protects possession, in order to succeed, action may have to be brought by the Internet café owner or staff and not the person to whom the information relates who, in the circumstances, would be a mere licensee.

3.2.2.1.2.2 Nuisance

Where there is an undue interference, (for a substantial length of time), with the use or enjoyment, of a person's property, an action in nuisance will lie.⁴²⁰ For an action based on nuisance to succeed, the plaintiff must have a legitimate interest in such property, in most cases, ownership.⁴²¹

However, in *Khorasandjian v Bush*,⁴²² where the plaintiff was constantly disturbed by persistent and unwanted phone calls, the Court of Appeal gave judgment for the plaintiff in respect of the defendant's harassment, based on the tort of private⁴²³ nuisance. This was in effect an extension of the tort of private nuisance, to cover an instance where the plaintiff has no interest in the land. This decision has however, been overruled in part. In

⁴²⁰ *Bone v Seale* [1975] 1 WLR 797, *Cunard v Antifyre Ltd* [1933] 1 KB 551 (See Talbot J at 556-7). See generally M R Brazier, D Alexander, R A Buckley, A S Burrows, H F Carty, A M Dugdale, M Mulholland, A Tettenborn, Lord Wedderburn of Charlton (eds) *Clerk & Lindsell on Torts* (1995) at 889.

⁴²¹ *Malone v Laskey* [1907] 2 KB 141. In *Oldham v Lawson* [1976] VR 654, the action was brought by husband and wife for nuisance, even though he had a legitimate interest as a licensee, the husband was held not eligible to sue as the house was owned by the wife.

⁴²² [1993] QB 727 (CA).

⁴²³ While any member of the public affected by the act complained about may bring an action for public nuisance, only a person with interest in property can successfully bring an action for private nuisance. Cf *Hunter v Canary Wharf Ltd* [1997] AC 655 at 690-4.

Hunter v Canary Wharf Ltd,⁴²⁴ the House of Lords re-established the principle that only a person with an interest in land can sue for private nuisance.

In *Read v J Lyons & Co Ltd*,⁴²⁵ nuisance was described as an “invasion of proprietary or other interest in land”. It has been said that any act of interference that amounts to intimidation, obstruction or violence will be an actionable nuisance and that to subject a person to watching and besetting so as to compel him to act in a particular way would be an actionable nuisance.⁴²⁶

The question would be whether such an act would qualify as an interference *stricto sensu* if the plaintiffs were not aware of its presence. It is suggested in this regard that the approach of the courts in *Christie v Davey*⁴²⁷ and *Hollywood Silver Fox Farm Ltd v Emmett*⁴²⁸ should be followed in affirming liability. In both *Christie*⁴²⁹ and *Hollywood*

⁴²⁴ Supra. See also Lord Goff at 698, and Lord Hoffmann at 706, who were of the opinion that instead of altering the elements of the tort of nuisance in *Khorasandjian*, the Court of Appeal should have tried to develop a new tort of harassment. Harassment is now actionable under the Protection from Harassment Act, (Chapter 40 of 1997), which came into force on June 16, 1997. See below at 68 & 69 for details on the Protection from Harassment Act.

⁴²⁵ [1947] AC 156, per Lord Simmons at 169-170.

⁴²⁶ See Brazier et al op cit at 893, Heuston & Buckley op cit at 86. In South Africa both the civil and criminal law recognise a cause of action for stalking: See *Epstein v Epstein* 1906 TH 87 (where the plaintiff was followed in public for a week); *R v Jungman* 1914 TPD 8 at 10,11 (where the complainant was continually and intentionally followed for ten minutes and also stared at); *R v Van Meer* 1923 OPD 77 (where the complainant was followed from place to place in a public library, followed out of the library and also stared at). See generally McQuoid-Mason op cit at 86-87.

⁴²⁷ [1893] 1 Ch 316.

⁴²⁸ [1936] 1 All ER 825.

⁴²⁹ Supra.

Silver Fox Farm,⁴³⁰ the defendants had acted deliberately and with malicious intent⁴³¹ and they were held liable for private nuisance in respect of acts that ordinarily would not constitute nuisance in the circumstances. This was because their conduct was an “abuse of rights.”⁴³²

In sum, where there has been interference with the quiet use and enjoyment of a person’s land by invading his or her privacy, for instance, watching from neighbouring premises or consistently telephoning the person’s home, protection may be found under the Common Law tort of nuisance. The tort of nuisance is usually associated with a continuing wrong or the maintenance of a state of affairs, and not a single act of the defendant.⁴³³ However, it has been held that in some instances, an action for nuisance may succeed where the act complained of is an isolated occurrence.⁴³⁴

⁴³⁰ *Supra*.

⁴³¹ In the Law of tort, except where there is an abuse of rights, motive or malice is generally irrelevant and does not ordinarily create liability where there would otherwise be none. Cf *Hollywood Silver Fox farm* Cf *Lunney and Oliphant* op cit at 604.

⁴³² See generally R Owen *Essential Tort Law* (2000) at 103. See also *Lunney and Oliphant* op cit at 604. In South Africa, action in such cases would be brought for abuse of rights. See MacDonald ACJ in *King v Dykes* 1971 (3) SA 540 at 545 “an owner must not use his land in a way which may prejudice his neighbours or the community in which he lives” See generally J C Van Der Walt *Delict: Principles and Cases* (1979) at 41-43. See also *McQuoid-Mason* op cit at 107, 112.

⁴³³ *SCM (UK) Ltd v Whittall & Son Ltd* [1970] 2 All ER 417, 430. In carrying out earth removal operations required in the construction of an aqueduct and reservoir for the city and the local water authority, a mechanical digger operated by one of the defendant’s men damaged an electric cable as a result of which current to the plaintiff’s business was interrupted. It was held that the escape of something on a single occasion would not necessarily constitute a nuisance unless the nuisance arose from the condition of the defendant’s land.

⁴³⁴ See *British Celanese Ltd v AH Hunt Capacitors (Ltd)* [1969] 1 WLR 959, *Spicer v Smees* [1946] 1 All ER 489. See also *Heuston & Buckley* op cit at 59-60.

3.2.2.1.2.2a Relevance to Internet Cafes

The Common Law tort of nuisance will be useful in the development of general principles for the protection of privacy in Nigeria as well as for the protection of Internet café privacy. Although the requirement for ownership excludes ordinary internet café users, (who are licensees) from successfully bringing action for acts occurring on the Internet café premises that may amount to nuisance, Internet café users may successfully bring action for nuisance where, for instance, they are being beleaguered at home with phone calls concerning information processed in an Internet café.

Internet café owners may also enjoy protection under the law of nuisance where they are being harassed with mail or phone calls in respect of any information processed in their Internet cafes.

3.2.2.1.2.3 Defamation

Defamation is concerned with injury to reputation⁴³⁵ resulting from words or images written, spoken, published, or otherwise expressed and also resulting from acts.⁴³⁶ It is

⁴³⁵ *Parmiter v Coupland* [1840] 6 M7 W 105 at 108, where Parke B laid down that the test as to whether a statement is defamatory is, whether the words complained of were calculated to injure the reputation of another. See also Lord Atkin in *Sim v Stretch* [1936] 52 TLR 669 at 671.

⁴³⁶ In *Hird v Wood* [1894] 38 Sol J 234, it was held that sitting near a placard and pointing at it with the finger amounted to (defamatory) publication. See also *Heuston & Buckley* op cit at 143-144, *Brazier et al* op cit at 1013.

the publication of a statement, which reflects on a person's reputation and tends to lower him or her in the eyes of right-thinking members of society.⁴³⁷

Liability for defamation may be divided into libel and slander.⁴³⁸ Slander is defamatory matter published in a transient form, often through the medium of spoken words,⁴³⁹ utterances or gestures,⁴⁴⁰ while libel consists of defamatory statements or representations in permanent form, such as writings,⁴⁴¹ paintings,⁴⁴² pictures,⁴⁴³ films⁴⁴⁴ and other forms of print,⁴⁴⁵ marks or signs exposed to view, waxwork effigies,⁴⁴⁶ statues,⁴⁴⁷ and other forms⁴⁴⁸ of publication.⁴⁴⁹

⁴³⁷ Per Lord Atkin in *Sim v Stetch* supra at 671. See also *Youssouppoff v Metro-Goldwyn-Mayer Pictures Ltd* [1934] 50 TLR 581, where the court held that to say that a woman had been raped would lower her in the eyes of right thinking members of the society, even though she was morally blameless. Cf *Byrne v Deane* [1937] 1 KB 818, where it was held that to suggest that someone had reported illegal activities to the police would not lower a person in the eyes of right thinking members of the community, as such the defendant's statement was not defamatory.

⁴³⁸ *King v Lake* [1667] 1 Hardres 470: See also Heuston and Buckley op cit at 143 & 144, Lunney & Oliphant op cit at 585.

⁴³⁹ *Gray v Jones* [1939] 1 All ER 795, where the defendant called the plaintiff a convicted person. See also *Bloodworth v Gray* [1844] 7 Man & G 334, where it was held to be slander to infer that a person has a contagious venereal disease; See also *Houseman v Coulson* [1948] 2 DLR 62.

⁴⁴⁰ In certain cases, it may not be easy to determine whether the appropriate cause of action is slander or libel. In *Youssouppoff v Metro-Goldwyn-Mayer Pictures Ltd* supra, where defamation was in form of words acted out in a film, it was held to constitute libel. Cf Heuston & Buckley op cit at 144.

⁴⁴¹ *Sutcliffe v Pressdram Ltd* [1990] 1 All ER 269, where the defendants published false allegations that the plaintiff, who was the wife of a murderer, had agreed to sell her story to a newspaper for 250,000 pounds. See also *Blackshaw v Lord* [1984] 1 QB 1.

⁴⁴² *Tolley v J S Fry and Sons Ltd* [1931] AC 333. Cf *McQuoid-Mason* op cit at 209.

⁴⁴³ *Cassidy v Daily Mirror Newspapers Ltd* [1929] 2 KB 331.

⁴⁴⁴ *Youssouppoff v Metro- Goldwyn- Mayer Pictures Ltd* supra, where the defendants implied in a film, that the plaintiff had been raped by a monk.

⁴⁴⁵ In *Godfrey v Demon Internet Ltd* [1999] 4 All ER 342; [2001] QB 201, an Internet service provider was held responsible in libel for material carried on its computers. Cf *Zeran v America Online* 129 F. 3d 327

In *Godfrey v Demon Internet Ltd*,⁴⁵⁰ the posting of defamatory material on the defendants website was held to be an actionable publication. The originator of defamatory material will also be liable for the repetition of defamatory information based on his or her defamatory publication, where such originator authorised the republication, or could have reasonably foreseen the repetition of the allegations contained in the original publication.⁴⁵¹

In this regard, it has been established that where defamatory material is accessed on an Internet Service Provider's newsgroup or stored in a newspaper's Internet archive, for each time that the material is accessed, there is an actionable publication for which the Internet Service Provider or newsgroup will be liable.⁴⁵²

The tort of defamation affords protection for the right to privacy where a person is portrayed in a false light or in cases where a person's name, image or likeness is

(4th Cir. 1997) where a United States court held that an Internet Service provider was not liable for defamatory messages published on its website by an unidentified third party.

⁴⁴⁶ *Monson v Tussauds Ltd* [1894] 1 QB 671 where an effigy of the plaintiff against whom a charge of murder was "not proven" was placed close to those of convicted murderers.

⁴⁴⁷ See Lopes J in *Monson v Tussauds Ltd* supra at 692.

⁴⁴⁸ See *Hird v Wood* supra.

⁴⁴⁹ See *Huth v Huth* [1915] 3 KB 32, Cf *Theaker v Richardson* [1962] 1 WLR 151.

⁴⁵⁰ Supra.

⁴⁵¹ In *Slipper v British Broadcasting Corporation* [1991] 1 QB 283, the defendants, a television company were held liable for defamatory comments contained in newspaper and magazine reviews of aspects of the life of the plaintiff, which were based on allegations contained in a preview that the defendants had shown to the press. Cf *McManus v Beckham* [2002] 1 WLR 2982.

⁴⁵² *Godfrey v Demon Internet Ltd* supra; *Loutchansky v Times Newspapers Ltd (No 2)* [2002] QB 783.

appropriated in a manner that lowers their reputation.⁴⁵³ It has been observed that, although the tort of defamation mainly protects pecuniary interests, the interests of dignity are also weighted heavily by the law in giving protection based on defamation.⁴⁵⁴

In *Archbold v Sweet*,⁴⁵⁵ where the defendants published a third edition of the plaintiff's work on criminal law without stating that it had not been edited by him, the plaintiff recovered damages on the grounds that the publication was capable of a defamatory meaning which could damage his reputation. Similarly in *Tolley v J S Fry*⁴⁵⁶ the plaintiff was awarded damages on the grounds that the publication was capable of a defamatory meaning, which could damage his amateur status as a golfer. In these cases, it is clear that the main interest protected by the law was the plaintiff's dignity and name.

There are, however, circumstances under which there will be no liability for defamation, and the court will not restrain publication of an article even though it is defamatory.

These include cases where the plaintiff has consented to the action of the defendant,⁴⁵⁷

⁴⁵³ *John V MGN* [1997] QB 586, where a newspaper article alleged that the plaintiff, a well-known entertainer, was addicted to a dangerous diet, and to support their claims, the defendants stated that the plaintiff had been watched at a Hollywood Christmas party.

⁴⁵⁴ Cf *McQuoid-Mason* op cit at 209.

⁴⁵⁵ [1832] 5 C 7 P 219; See also *Ridge v The Illustrated English Magazine* [1913] 29 TLR 592.

⁴⁵⁶ *Supra*. Cf *McQuoid-Mason* op cit at 209.

⁴⁵⁷ *Cookson v Harewood* [1932] 2 KB 478n; 101 LJKB 394n, where the plaintiff had submitted to the rules of a club, one of which was that the stewards of the club might warn off anybody. The defendants subsequently published a true statement that the plaintiff had been warned off all pony racing tracks under their control. The defendants were held not liable as they had published a true statement and the defendants had authority to make the publication.

where there is justification for the defendant's comments,⁴⁵⁸ where it is a fair comment on a matter of public interest⁴⁵⁹ and where the statement made is privileged.⁴⁶⁰ It must also be noted that the Defamation Act⁴⁶¹ contains extensive provisions regulating the law of defamation.⁴⁶²

3.2.2.1.2.3a Relevance to Internet Cafes

In applying the above, it may be affirmed that an Internet café owner will be liable for defamatory material where s/he is the originator of a defamatory message, authorizes such defamatory message, or refuses to remove a defamatory message from their website, or from their archives.

Although Internet cafes in Nigeria do not usually function as Internet Service Providers,⁴⁶³ or have personalized websites and as such, may not ordinarily be liable for publication in these respects, the principle in *Godfrey v Demon Internet Ltd*,⁴⁶⁴ is relevant in extending liability to Internet café owners for publication where they carry

⁴⁵⁸ *Williams v Reason* [1988] 1 WLR 96.

⁴⁵⁹ *Bonnard v Perryman* [1891] 2 Ch 269, CA, see also Lord Finlay in *Sutherlands v Stopes* [1925] AC 47 at 62, 63.

⁴⁶⁰ *Minter v Priest* [1930] A.C. 558, *Angel v Bushell Ltd* [1968] 1 QB 813.

⁴⁶¹ Chapter 66 of 1952 as amended by the Defamation Act (Chapter 31 of 1996). See below Para 3.2.2.1.2.

⁴⁶² See below Chapter 3.

⁴⁶³ All the Internet cafes visited relied on third party Internet Service Providers; none were, themselves, Internet Service Providers.

⁴⁶⁴ *Supra*.

defamatory matter and do not act to remove it. For instance, where a library or bookstore knows it is carrying defamatory matter and does not act to remove it, if the material is subsequently circulated and or published directly through the library or bookstore, they may become liable for publication.

Thus, although Internet café owners will ordinarily not be held liable for defamatory messages sent or received by third parties in their café if the Internet café owner did not authorize or originate the defamatory message, they may become liable for a defamatory message not originating from, or authorized by them, if, after being instructed to delete or remove the message, the owner does not comply.

3.2.2.1.2.4 Malicious Falsehood

The tort of malicious falsehood is closely related to the tort of defamation. However the elements to be proved for the two torts are different. While malice must be present and the statement complained of false, before an action in malicious falsehood can succeed,⁴⁶⁵ injury to reputation, and not malice, must be proved in a defamation action.⁴⁶⁶

Conversely, in an action for malicious falsehood it is not required that the plaintiff suffer injury to reputation. Economic harm to the plaintiff is sufficient.⁴⁶⁷

⁴⁶⁵ *Joyce v Sengupta* [1993] 1 All ER 897 (CA). Cf *Brazier et al op cit* at 1157.

⁴⁶⁶ Cf *Godfrey v Demon Internet Ltd supra*.

⁴⁶⁷ Cf *Brazier et al op cit* at 1157, 1160.

In *Joyce v Sengupta*,⁴⁶⁸ the plaintiff's action for malicious falsehood in respect of newspaper reports that she had stolen personal letters from her employers succeeded. The tort also provides limited protection for the right to privacy where false or misleading information is intentionally and wrongfully, or, maliciously published about a person in circumstances that they cause economic harm to the plaintiff.⁴⁶⁹

In *Kaye v Robertson*,⁴⁷⁰ where the plaintiff was interviewed and photographed when he was not in a fit condition to do the interview or give informed consent to the interview, the court granted an interlocutory injunction to prevent the defendants from publishing anything that might be understood to mean that the plaintiff had voluntarily consented to the interview and the taking of the photographs. The tort of malicious falsehood protects interests similar to those protected in false light privacy cases. However, for the tort of malicious falsehood, malice must be shown in the defendant's action.

3.2.2.1.2.4a Relevance to Internet Cafes

This tort may be relied on by Internet café users where the defendant maliciously or wrongfully publishes false or misleading information about the plaintiff on the basis of information obtained through Internet café sources, resulting in economic harm to the plaintiff.

⁴⁶⁸.Supra.

⁴⁶⁹ See generally Brazier et al op cit at 1157, 1160.

3.2.2.1.2.5 Passing-off

The tort of passing-off is also similar to the tort of defamation. An action for passing-off will lie where in the course of his or her business a person represents his or her goods as those of another in a manner calculated to deceive members of the public into thinking that such goods are those of that other.⁴⁷¹

In *Reckitt & Colman (Products) Ltd v Borden Inc.*,⁴⁷² it was held that the shape, colour, decoration, packaging, by means of which goods or business premises are identified, could become well enough known as those of a particular trader for use of that get-up to amount to passing off. Passing-off is however limited to persons engaged in a field of common business activity.⁴⁷³ The tort of passing-off protects the right to privacy where the defendant's action of passing-off places the plaintiff in a false light.

3.2.2.1.2.5a Relevance to Internet Cafes

This will only be relevant where both parties process business information via computers in Internet cafes. Where an Internet café user processes information relating to his or her

⁴⁷⁰ [1991] FSR 62.

⁴⁷¹ *Hines v Winnick* [1974] Ch. 708, see Vaisey J at 713; *Lord Bryon v Johnston* (1816) 35 ER 851 where Lord Bryon was able to prevent the publication of poems falsely attributed to him on the basis of this action. See also Brazier et al op cit at 1403, Heuston & Buckley op cit at 395. See also *Sim v Heinz* [1959] 1 All E.R. 547.

⁴⁷² [1990] 1 WLR 491 (HL).

⁴⁷³ *Sim v Heinz* supra where the action could not be invoked by a well-known actor to restrain another from imitating his voice in a television commercial. Cf *Sim v Stretch* (1936) 52 TLR 669; See also *Kaye v Robertson* supra, *Granada Group Ltd v Ford Motor Co Ltd* [1972] FSR 103.

business, for instance, the design or label for their products, or a business logo, in an Internet café and another user copies or imitates the label, design or logo, the first party may successfully bring an action for the tort of passing off in respect of the unlawful use of business information by the latter.

3.2.2.1.2.6 Intentional Infliction of Emotional Injury

The tort of intentional infliction of emotional injury may be said to be a type of trespass to person for which relief is available where the plaintiff's peace of mind or emotional well-being is disturbed by the action of the defendant.⁴⁷⁴ In *Wilkinson v Downton*,⁴⁷⁵ the plaintiff's peace of mind was disturbed by a false report that her husband had been badly injured in a collision. Similarly, where the plaintiff was told, by private detectives, that unless she procured certain letters from her mistress, they would publicly disclose that her fiancée had been interned during World War 1 as a traitor, the defendants were held liable for intentional infliction of distress.⁴⁷⁶

It must be noted that, although the first few cases on this tort involved false statements, it would appear that successful action can be brought for intentional infliction of harm, where the defendant's statement is true; the law does not weigh the veracity of the

⁴⁷⁴ See *Wilkinson v Downton* [1897] 2 QB 57.

⁴⁷⁵ *Supra*.

⁴⁷⁶ *Janvier v Sweeney*[1919] 2 KB 316.

defendant's statement, but the result of his or her action.⁴⁷⁷ This tort affords some protection for the right to privacy where the act of the defendant threatens the plaintiff's health.⁴⁷⁸ Thus in *Burnett v George*⁴⁷⁹ where the plaintiff was relentlessly harassed by a former boyfriend, the court held that the defendant's conduct fell within the tort defined in *Wilkinson v Downton*.⁴⁸⁰

3.2.2.1.2.6a Relevance to Internet Cafes

This tort will be of utility for the protection of privacy in Internet cafes where there is increased potential for Internet café owners, their staff, and, or, other users to access information relating to others. The tort will afford protection where an Internet café owner or any other person uses information obtained via an Internet café to threaten, blackmail, or otherwise harass the plaintiff, resulting in physical or psychological harm to him or her.

3.2.2.1.3 Conclusion on Common Law Protection of Privacy in the United Kingdom

⁴⁷⁷ See Lunney & Oliphant op cit at 54,55. According to them, this tort is available in respect of "intentional acts the inevitable consequence of which is physical (or psychological) harm" (at 54). Cf W V H Rogers (ed.) *Winfield & Jolowicz on Tort* (1994) at 17, 74.

⁴⁷⁸ See also *McLoughlin v O'Brian* [1983] 1 AC 410; *Vernon v Bosley* [1997] 1 All ER 577. See generally Lunney & Oliphant op cit at 56, 275ff.

⁴⁷⁹ [1992] 1 FLR 156.

⁴⁸⁰ (Supra).

It can be seen that Common Law torts cover both areas of family/domestic, and business situations. While the torts of trespass and nuisance afford protection for privacy in family situations, such torts as passing-off and defamation protect the right to privacy in business situations. Furthermore, the equitable remedy of breach of confidence affords protection for the right to privacy in both family and business situations. More specifically, breach of commercial confidence protects the right to privacy in business situations.⁴⁸¹

It is nevertheless clear that Common Law protection of the right to privacy is limited. It must be noted however, that the position concerning the protection of privacy in the United Kingdom has changed with the coming into effect of the Human Rights Act⁴⁸² and it is expected that better privacy protection will be available in the United Kingdom as the courts uphold the principles in the Act.⁴⁸³

With regard to the protection of electronic mail privacy in Internet cafes, it has been shown that the law relating to breach of confidence and certain torts will be useful. The applicable torts and breach of confidence principles will be referred to later in this work to formulate general principles for the protection of e-mail privacy in Nigeria. However, the English Common Law torts and the breach of confidence laws considered above do not provide comprehensive protection for e-mail privacy. Thus, the need remains to look further for better protection for this in the context of data protection laws.

⁴⁸¹ *Reckitt & Colman (Products) Ltd v Borden Inc* supra.

⁴⁸² Chapter 42 of 1998.

3.2.2.2 Common Law Protection of Data in the United Kingdom

There are no direct provisions on data protection under the English Common Law.⁴⁸⁴ It does not contain any provisions regarding information contained in a data bank, computerised pools of information, who may collect data and for what purposes, neither does it provide for the accuracy or accessibility of such data.⁴⁸⁵ Where, however, the use or disclosure of information amounts to a breach of confidence or falls under the purview of certain nominate torts, a plaintiff may find redress.⁴⁸⁶ There is an obvious *lacuna* here. It is therefore necessary to look at statute law for solutions.

3.2.3 Statutory Protection of Privacy and Data in the United Kingdom

3. 2. 3. 1 Statutory Protection of Privacy

3.2.3.1. 1 The Human Rights Act

The Human Rights Act⁴⁸⁷ incorporates certain provisions of the European Convention on Human Rights into the domestic law of the United Kingdom. Prior to the coming into

⁴⁸³ See below Para 3.2.2.1.1ff.

⁴⁸⁴ See McQuoid-Mason op cit at 55ff.

⁴⁸⁵ Ibid.

⁴⁸⁶ Ibid.

⁴⁸⁷ Chapter 42 of 1998.

effect of the Human Rights Act, an applicant could appeal to the European Court of Human Rights provided he or she had exhausted the available domestic law remedies.

In *Earl and Countess Spencer v United Kingdom*,⁴⁸⁸ the European Commission held that the application was inadmissible because the applicant had not exhausted the available domestic remedies. The court said that the applicants had not demonstrated that the remedy of breach of confidence, which was available, was insufficient or ineffective. The plaintiffs' application was inadmissible.

In *Winer v United Kingdom*,⁴⁸⁹ the applicants sought protection under Article 8 for the publication of a book containing both true and false information about them. The Commission denied the applicants' claim partly on the ground that there were sufficient causes of action in national law for the plaintiffs to bring action. In this case, the Commission was of the opinion that law of defamation was sufficient to provide remedy in respect of the publication of the information that was false. (The Commission was reluctant to grant remedy for publication of the true information as this would curtail the right to freedom of expression provided for in Article 10.)

⁴⁸⁸ Applications Nos 28851/95 and 28852/95. Commission decision of 16 January 1998 (DR 92-A p56).

⁴⁸⁹ (1986) 48 DR 154.

In line with this decision it has been suggested that the action for breach of confidence is sufficiently broad to accommodate cases of invasions of privacy, and accordingly may be developed to protect privacy.⁴⁹⁰

With the coming into effect of the Human Rights Act,⁴⁹¹ there is no longer a need to rely on the nominate torts for the protection of the right to privacy, as it is now provided for in the domestic law.⁴⁹² Section (2) 1 of the Human Rights Act provides that the courts must consider judgements, decisions, declarations, and advisory opinions of the European Court of Human Rights, as well as other relevant opinions and decisions as set out in Section (2) 1 (b)-(d). In essence, the courts must recognise and give effect to the right to privacy as set out in the Convention.

Article 8 of the European Convention on Human Rights, (subsequently referred to as the ECHR) expressly provides for the right to privacy. Article 8 guarantees the right to respect for private and family life, home and correspondence,⁴⁹³ and also prohibits the interference of public authorities with the exercise of this right.⁴⁹⁴

⁴⁹⁰ G Phillipson & H Fenwick "Breach of Confidence as a Privacy Remedy in the Human Rights Act Era" 63 *Modern Law Review* (2000) at 693.

⁴⁹¹ Chapter 42 of 1998.

⁴⁹² See *Douglas v Hello! Ltd* [2001] QB 967, [2002] 1 FCR 289, [2003] EWHC 786. Cf below at 110.

⁴⁹³ Article 8(1).

⁴⁹⁴ Article 8(2).

It has been said that the scope of protection of Article 8 of the ECHR is wide and covers control over personal information and freedom from intrusion;⁴⁹⁵ identity;⁴⁹⁶ sexual intimacy (with regard to the protection of private life)⁴⁹⁷; children born out of wedlock (with regard to the protection of family life),⁴⁹⁸ and the place where one intends to live (with regard to the protection of the home).⁴⁹⁹

The provision protecting correspondence has been interpreted to protect both personal and business correspondence,⁵⁰⁰ and includes telephone correspondence, as well as post.⁵⁰¹ It has also been suggested that the provision may be extended to cover electronic mail.⁵⁰²

⁴⁹⁵ *Niemetz v Germany* (1992) 16 EHRR 97, *Malone v United Kingdom* (1984) 7 EHRR 14 (on unlawful police searches and telephone tapping).

⁴⁹⁶ See *B v France* (1992) 16 EHRR 1, *Cossey v United Kingdom* (1990) 13 EHRR 622, *Rees v United Kingdom* (1986) 9 EHRR 56 (on the rights of transsexuals to have their change of identity recognised by the State).

⁴⁹⁷ *Dudgeon v United Kingdom* (1981) 4 EHRR 149 (on the rights of homosexuals to engage in consensual acts between adults in private); See generally *Niemetz v Germany* supra at para 29. It has been observed, S Foster “The Right to Private Sexual Life under Article 8 of the European Convention on Human Rights: ADT v U.K.” 35 *Law Teacher*, (2001) No 1 at 81f, that the courts in the United Kingdom have shown a tendency to interpret Article 8(2) conservatively with regard to privacy involving homosexual acts; Cf *Laskey, Jaggard & Brown v United Kingdom* (1997) 24 EHRR 39, *Smith & Grady v U.K* (2000) 29 EHRR 493. In *Laskey*, the court held that the presence of other people during the consummation of the sexual acts and the fact that the sexual acts were video-taped took the acts outside the scope of “private life” as provided by Article 8.

⁴⁹⁸ *Marckx v Belgium* (1979) 2 EHRR 330, where the court found legislation that discriminated against children born outside wedlock to be in violation of Art. 8.

⁴⁹⁹ *Gillow v United Kingdom* (1986) 11 EHRR 335; *Buckley v United Kingdom* (1994) 18 EHRR 191.

⁵⁰⁰ *Niemetz v Germany* supra.

⁵⁰¹ *Klass v Germany* supra.

⁵⁰² A Nicol, G Millar, A Sharland *Media Law and Human Rights* (2001) at 88.

In the light of the above, decisions such as *Kaye v Robertson*,⁵⁰³ *R v Brent London Borough Council, ex p Peck*,⁵⁰⁴ and *R v Khan*⁵⁰⁵ which rejected a right to privacy in English law, are likely to be overruled.

In *Douglas v Hello! Ltd*⁵⁰⁶ the defendants took un-authorised photographs of the plaintiffs' wedding and they attempted to publish the pictures. The Court of Appeal, stating that it had taken into account the provisions of the Human Rights Acts and Section 8 of the European Convention on Human Rights,⁵⁰⁷ affirmed that the plaintiffs had a right to privacy, which English law would recognise and protect.⁵⁰⁸ The plaintiffs were granted an interdict prohibiting publication of the wedding photos.

However, the scope of the right to privacy guaranteed in the Convention is also limited by the recognition of other rights, especially the right to freedom of expression, which is guaranteed in Article 10 of the ECHR. In this regard, the European Court of Human Rights has said that freedom of the press is an essential foundation of a democratic society.⁵⁰⁹

⁵⁰³ Supra. Although, in this case, the plaintiff found some protection under the tort of malicious falsehood, the protection was limited as the defendants were still allowed to publish the information. See above Para 3.2.1.2.4.

⁵⁰⁴ (1997) *Times Law Reports* 18 December; See above Para 2.3.1.1.

⁵⁰⁵ [1997] AC 558.

⁵⁰⁶ Supra.

⁵⁰⁷ At Paragraph 3.

⁵⁰⁸ Per Sedley L.J. Para 125

⁵⁰⁹ See *Sunday Times v United Kingdom* (1979-80) 2 EHRR 245.

In *Campbell v MGN Ltd*,⁵¹⁰ where the defendant newspaper unlawfully published personal information about the drug addiction of a famous fashion model, the Court of Appeal ruled that the publication of the story and picture were in the public interest and that the defendants had acted justifiably in the light of their right to freedom of expression guaranteed in Article 10. Here, it appears that the plaintiff would have been able to recover had the publication not been in the public interest.

It has also been observed that under the provisions of Article (8)2 which prohibit interference by public authorities,⁵¹¹ liability for infringements may be avoided where there is justification, and this has raised a doubt as to whether the provision can be invoked where there is a violation of privacy by the media or a private investigator.⁵¹² In this regard, it has been suggested that the positive obligation imposed on states by Article 8 may require legal regulation of the collection and use of personal information by private agencies.⁵¹³

This is illustrated in *Halford v United Kingdom*,⁵¹⁴ where the applicant's office telephone was monitored. The court held that the absence of Civil law regulation of the monitoring

⁵¹⁰ [2003] QB 633.

⁵¹¹ This has been described as negative obligation (to refrain) imposed by the Act. See generally J Wadham & H Mountfield *Blackstone's Guide to the Human Rights Act 1998* (1999) at 92. In *Dudgeon v United Kingdom* supra the court found legislation that criminalized all homosexual behaviour to be in violation of Article 8. See also *X v United Kingdom*. (1997) 24 EHRR 143.

⁵¹² E Barendt "Privacy as a Constitutional Right and Value" in P Birks (ed.) *Privacy and Loyalty* (1997) at 12.

⁵¹³ D Feldman "The Developing Scope of Article 8 of the European Convention on Human Rights" [1997] *EHRLR* 266 at 272.

of internal telephone systems, (even though there were police internal codes of practice), did not comply with Article (8)2 of the Convention, and that there had been a violation of the applicant's right under Article 13 to have an effective remedy in national law for breach of her rights under Article 8.⁵¹⁵

In addition to section 2(1) which the courts, Section 8 of the Human Rights Act also provides that the courts may grant any relief or remedy or make any order that it considers just and appropriate for breaches of the ECHR as long as such remedy, relief or order is within the powers of the court to award. Section 8(4) of the Act provides that in determining whether to award damages or the amount of an award, the courts must take the principles applied by the European Court of Human Rights into account. In effect, it appears that the courts in the United Kingdom have a measure of freedom to develop a law of privacy using cases from the European Court of Human Rights as a foundation.

The European Court of Human Rights has held⁵¹⁶ that Article 8 imposes a positive obligation to respect privacy and that the obligation imposed extends to protect an individual from the acts of other private parties.⁵¹⁷ Thus, it appears that the provisions of the Human Rights Act will apply both vertically (between the State and individuals) and horizontally (between individuals).

⁵¹⁴ (1997) 24 EHRR 523 at Para 51, See also *Malone v United Kingdom* supra.

⁵¹⁵ It must be noted that the Interception of Communications Act (1985) regulates the monitoring of calls on public networks, and does not apply to internal monitoring of calls. The Act creates criminal offences, but does not directly affect the law of tort. See A M Dugdale (General ed.) *Clerk and Lindsell on Tort* (2000) at 1527; Heuston and Buckley op cit at 37.

⁵¹⁶ *X and Y v The Netherlands* (1986) 8 EHRR 235 Para 23.

⁵¹⁷ Cf *Douglas v Hello! Ltd* supra; *Campbell v MGN Ltd* supra.

It has however been noted⁵¹⁸ that Convention rights cannot be directly enforced in proceedings against private litigants. The only effect that the Act will have in such cases is an indirect one arising from the interpretative obligations imposed on the court by section 3.

Section 3 of the Human Rights Act provides that all legislation (past and future) must be read and given effect to in a way that is compatible with the Convention. This section, however, further provides that the obligation to interpret legislation compatibly with the Convention “does not affect the validity, continuing operation or enforcement of any incompatible” primary or subordinate legislation. In essence, although the provisions of the Human Rights Act may effectively override and change existing Common Law,⁵¹⁹ the courts are bound to uphold and apply Acts of parliament and other subordinate legislation even where they are inconsistent with the provisions of the Convention.

In support of the position that the courts may be bound to uphold legislation that is incompatible with the Convention, Section 4 provides that where it is not possible to give effect to the obligation in a way that is compatible with Convention rights, a competent court must consider the option of making a declaration of incompatibility.⁵²⁰ Such a declaration does not affect the validity, continuing operation or enforcement of the

⁵¹⁸ Wadham & Mountfield *op cit* at 3.

⁵¹⁹ *Cf Douglas v Hello! Ltd supra*.

⁵²⁰ Section 4. See generally S Grosz, J Beatson, P Duffy *Human Rights The 1998 Act and the European Convention* (2000) at 28ff. Incompatibility with the Convention rights occurs “where it is impossible to comply with both the requirements of a U.K. statute and those of the Convention”; For example, “where there is express contradiction between statute and Convention rights”. (Grosz et al *op cit* at 39).

provision in respect of which it is made.⁵²¹ It may however prompt Parliament to consider amendments in respect of the legislation in question.⁵²² In effect, the courts cannot on their own apply or effect any amendment to legislation where such legislation is incompatible with the provisions of the Convention; they are bound to apply legislation “as is” until an amendment is made by parliament.

Further to this, Section 6 provides that all public authorities, including the courts, must comply with the Convention unless a statute positively prevents this. In essence, the courts will only be able to apply the principles in the Convention and the Human Rights Act to effect any change to the existing law of privacy where there is no legislation providing to the contrary. Where there is any inconsistency between the provisions of the Convention and those of a statute, the statute shall override the Convention to the extent of the inconsistency.

Where, however, there has been an invasion of privacy in breach of the principles of human rights, in circumstances where United Kingdom legislation prevents compliance with the Convention, (or essentially disregards or detracts from the protection available for a complainant in accordance with international human rights principles) an aggrieved person would be able to institute action in the European Court of Human Rights.

⁵²¹ Section 4(6). See also Grosz et al op cit at 56.

⁵²² Grosz et al op cit at 56, Wadham & Mountfield op cit at 193.

From the above, it is clear that parliamentary sovereignty will not be compromised in the United Kingdom and that validly-made legislation overrides all other laws, including the international human rights principles that have been incorporated into local law, and provisions of International Conventions.⁵²³

It is submitted that this situation constitutes a breach of the Convention and detracts from the force of the incorporated provisions of the Convention and the Human Rights Act. The principle of parliamentary sovereignty whereby Parliament has unlimited powers has been greatly criticised.⁵²⁴

With regard to the right to privacy, it has been suggested that the restrictions contained in sections 3, 4 and 6 of the Act, should not narrow the scope of the protection afforded to privacy beyond those recognised by the ECHR, and that since the right provided for in Article 8 is qualified, issues of incompatibility should hardly arise.⁵²⁵

It is submitted that whether the right guaranteed in Article 8 of the Act is qualified or general, the possibility remains of enacting parliamentary laws that are incompatible with

⁵²³ The Human Rights Act is intended to maximise “the position of human rights without trespassing on parliamentary sovereignty” (*Hansard*, H.L., November 3, 1997, col.1229), and to “be consistent with the sovereignty of parliament as traditionally understood” November 18, 1997, col. 522; See also *Hansard*, H.L. February 5, 1998, col 89 “The sovereignty of parliament should not be disturbed.” See generally Grosz et al op cit at 30ff. See also Wadham & Mountfield op cit at 3 & 4.

⁵²⁴ See Grosz et al op cit at 31. Cf P Craig “The Courts, The Human Rights Act and Judicial Review” 117 *Law Quarterly Review* October (2001) at 596ff.

⁵²⁵ Grosz et al op cit at 39, where it is observed that the provisions of Article 8(2) of the Act are not likely to give rise to contradictions arising from the text of the provision as the right guaranteed is qualified and not general (or absolute).

the provisions of the Convention such that the rights guaranteed by the Convention are rendered of virtually no effect.⁵²⁶ The position therefore is that although past acknowledgement of a need for privacy law⁵²⁷ and recent application of the Human Rights Act⁵²⁸ by the courts are positive indicators, it still remains to be seen what impact the restrictions in sections 3 and 6 of the Human Rights Act will have on the right to privacy, and, to what extent the rights guaranteed in Article 8 will be limited by these provisions.

3.2.3.1.1a Relevance of the Human Rights Act to the Protection of Privacy in Internet Cafes in Nigeria

With regard to the protection of electronic mail in Internet cafes, it is noteworthy that the Nigerian Constitution contains privacy protection provisions comparable to those in the Convention. These provisions have however not received much attention in terms of litigation or, and, judicial interpretation. The generous interpretation of Article 8 of the European Convention on Human Rights, which covers control over personal information, freedom from intrusion,⁵²⁹ as well as other sensitive aspects of private life⁵³⁰ will be

⁵²⁶ Cf the United States of America PATRIOT Act below Para 4.3.1.13.

⁵²⁷ Laws J in *Hellewell v Chief Constable of Derbyshire* supra at 807; Glidewell LJ at 66, Legatt LJ at 71 in *Kaye v Robertson* supra; See also Lord Denning *House of Lords' Debates* (1961) Vol 229 Col 638.

⁵²⁸ *Douglas v Hello!* Supra; See above Para 3.2.2.1.1.

⁵²⁹ *Malone v United Kingdom* supra.

⁵³⁰ For instance, children born out of wedlock: *Marckx v Belgium* supra; sexual intimacy: *Dudgeon v United Kingdom* supra. See above Para 3.2.3.1.1.

useful and should be referred to for guidance in construing and applying the Nigerian provisions.

Although Nigeria is not a signatory to the Convention and as such, the courts may not ordinarily be bound to consider and apply the Convention principles, based on Nigeria's history of reliance on English Common law, it is suggested that changes in English (Common) law reflecting advance or progress should at the least be considered of persuasive import in Nigeria. In this regard, it is suggested that the privacy provisions of the European Convention as adopted into the United Kingdom Human Rights Act should be given due consideration and applied where relevant in Nigeria.

The broad interpretation given to the provision protecting correspondence⁵³¹ will be particularly instructive for the protection of electronic mail privacy and for the protection of data generally.

3.2.3.1.2 Other Statutes

There are other statutory provisions in which protection of the right to privacy may be found. Some of these are the Interception of Communications Act of 1985,⁵³² the Police

⁵³¹ Correspondence has been interpreted to protect personal as well as business correspondence, telephone and possibly e-mail correspondence. Cf above Para 3.2.2.1.1.

⁵³² Chapter 56.

Act 1997,⁵³³ the 1952 Defamation Act,⁵³⁴ the 1996 Defamation Act,⁵³⁵ and the Protection from Harassment Act 1997.⁵³⁶

3.2.3.1.2.1 The Interception of Communications Act of 1985⁵³⁷

The Interception of Communications Act of 1985⁵³⁸ sets limitations on surveillance of telecommunications. The Act makes it an offence to intercept communications sent through the post and telecommunication system, without authorisation by the Secretary of State.⁵³⁹ The Act also specifies conditions under which a warrant may be issued.⁵⁴⁰ The Police Act 1997⁵⁴¹ also contains provisions regulating police interception of confidential material.⁵⁴² The Act requires authorisation from a Commissioner for the use by the police of listening devices.⁵⁴³

⁵³³ Chapter 50.

⁵³⁴ Chapter 66.

⁵³⁵ Chapter 31.

⁵³⁶ Chapter 40.

⁵³⁷ Chapter 56.

⁵³⁸ Chapter 56.

⁵³⁹ Section 1. See *Christie v United Kingdom* (1994) 78-A DR 119.

⁵⁴⁰ Section 2(2).

⁵⁴¹ Chapter 50.

⁵⁴² Section 97.

⁵⁴³ *Ibid.*

3.2.3.1.2.1a Relevance to Internet Cafes

The regulation of interception of communications is a germane issue in the protection of Internet communication. Legislation regulating interception, not only of Internet communications, but all radio communication is a necessity for effective privacy and data protection. As of July 2006, it was estimated that there were about 16 million cellular-phone users in Nigeria⁵⁴⁴ and, as established earlier on,⁵⁴⁵ the processing of information in Internet cafes is common in Nigeria. Until 2005, Nigeria had no general legislation equivalent to the Interception of Communications Act of 1985 in terms of the protection of privacy and data.⁵⁴⁶ Recently however, a bill⁵⁴⁷ for the protection of information contained in computers has been passed.

The Computer Security and Critical Information Infrastructure Protection Bill⁵⁴⁸ contains provisions regulating access to computer records. Section 2 of the Bill criminalizes unlawful or unauthorized access to any computer in order to secure access to a program or data held in the computer. Section 12 deals with interception of communications and

⁵⁴⁴Research and Markets; MobileAfrica <http://www.mobileafrica.net/a70.htm> Accessed January 2007.

⁵⁴⁵ Chapter 1 Para 1.4.

⁵⁴⁶The earliest telecommunications legislation in Nigeria was the Telegraphs Ordinance 1916, which provided for the regulation of the construction and the working of telegraph lines. This and subsequent legislation (The Wireless Telegraphy Ordinance [Cap 233 1948 Revised Edition of the Laws of Nigeria] have since been abolished/repealed. The Wireless Telegraphy Act No 31 of 1961 (as subsequently amended) replaced the Wireless Telegraphy Ordinance. Apart from the Wireless Telegraphy Act which contains some provisions limiting the obtaining and disclosure of information with the use of wireless telegraphy equipment (above at Para 7.2.2.2.3), none of these laws contains detailed or substantial provisions for the protection of privacy and data.

⁵⁴⁷ The Computer Security and Critical Information Infrastructure Protection Bill 2005.

makes it an offence to intentionally and without lawful authority, or in excess of authority intercept any communication processed in Nigeria.

The Bill also provides for the circumstances under which Service Providers, their employees and authorised agents may intercept communication.⁵⁴⁹ It also permits interception by law enforcement agencies⁵⁵⁰ and provides for circumstances under which such interception can be carried out.⁵⁵¹ Relevant provisions of the Computer Security and Critical Infrastructure Protection Bill will be discussed in greater detail below.⁵⁵²

The United Kingdom Interception of Communications Act⁵⁵³ will be useful as a reference point and provide some guidance in enacting effective legislation for the regulation of interception of communications in Nigeria.

3.2.3.1.2.2 The 1952 Defamation Act⁵⁵⁴ and the 1996 Defamation Act⁵⁵⁵

The 1952⁵⁵⁶ and 1996⁵⁵⁷ Defamation Acts contain detailed provisions on defamation. The 1996 Act repeals certain sections of the 1952 Act⁵⁵⁸ and also contains new provisions

⁵⁴⁸ 2005.

⁵⁴⁹ Section 12(2).

⁵⁵⁰ Section 12(3).

⁵⁵¹ Section 12(3)(a).

⁵⁵² Chapter 7 Para 7.2.2.1.

⁵⁵³ Chapter 56 of 1985.

⁵⁵⁴ Chapter 66 of 1952.

⁵⁵⁵ Chapter 31 of 1996.

⁵⁵⁶ Chapter 66 of 1952.

regulating certain aspects of defamation.⁵⁵⁹ By virtue of Section 1 of the 1996 Act, an Internet Service Provider, or Internet café owner may escape liability for the publication of defamatory materials on its system if such service provider or café owner can show that:

- (a) he [she, or it, in the case of an Internet service provider] was not the author, editor or publisher of the statement complained of;
- (b) he [she, or it] took reasonable care in relation to its publication; and
- (c) he [she, or it] did not know, and had no reason to believe, that what he [or she] did caused or contributed to the publication of a defamatory statement.⁵⁶⁰

Sections 8-10 of the 1996 Act provide for summary disposal of a plaintiff's claim. Where in an action for defamation the court is of the opinion that the defendant has no defence that is reasonably likely to succeed, and there is no other reason why the case should be tried, judgement may be given for the plaintiff.⁵⁶¹

Summary relief as set out by the Act includes a declaration that the statement was false or defamatory, an order that the defendant publish a suitable correction and apology, and an award of damages to the plaintiff.⁵⁶² Thus where a person's privacy is invaded by the

⁵⁵⁷ Chapter 31 of 1996.

⁵⁵⁸ For instance, Section 4 of the 1952 Act, which provides for a defence of unintentional defamation, has been repealed by Sections 2-4 of the 1996 Act.

⁵⁵⁹ Sections 2-4 of the 1996 Act create a defence of offer of amends by a person who has published a statement alleged to be defamatory. Sections 8-10 of the 1996 also provide for summary disposal of defamation claims.

⁵⁶⁰ Section 1 (a) –(c) Defamation Act Cap 31 of 1996.

⁵⁶¹ Section 8.

publication of material that may be regarded as defamatory under circumstances that fall within Section 8 of the 1996 Defamation Act, the plaintiff can obtain expeditious relief for such invasion of privacy under these provisions.

3.2.3.1.2.2a Relevance to Internet Cafes

Although the action for defamation is recognised in Nigerian tort law,⁵⁶³ it exists essentially in the form of old English Common Law applicable prior to the Defamation Acts.⁵⁶⁴ The Defamation Acts⁵⁶⁵ provide guidance for the protection of privacy in Internet cafes where an Internet Service Provider or Internet café owner is the author, editor or publisher of defamatory material, or did not take reasonable care in relation to the publication of defamatory material published. The Act will also be useful in cases where an Internet Service Provider or Internet café owner does an act or omission that contributes to the publication of defamatory material.

The provisions of Sections 8 to 10 of the Act on summary disposal of claims and summary relief may also be informative for the provision of expeditious relief in cases of Internet café publication of defamatory material where the court is not convinced that the defendant has a defence reasonably likely to succeed and in the absence of any other reason to proceed with the hearing of the case.

⁵⁶² Section 9.

⁵⁶³ Cf below Para 6.2.1.5.

⁵⁶⁴ Cf below Para 6.2.1.

⁵⁶⁵ Chapter 66 of 1952, Chapter 31 of 1996.

3.2.3.1.2.3 The Protection from Harassment Act 1997⁵⁶⁶

This Act creates a statutory tort that gives a right of action for harassment. The Act does not contain a definition of “harassment”. To harass a person has however been defined to mean “to annoy or worry somebody by putting pressure on them or saying or doing unpleasant things to them.”⁵⁶⁷ Section 1(1) of the Act provides that a person must not pursue a course of conduct that amounts to harassment of another and which he or she knows or ought to know amounts to harassment of another.

Section 7 (2) of the Act provides that harassing a person includes alarming a person or causing the person distress. There are however circumstances under which there will be no liability under the Act, for instance, where the course of conduct is pursued for the purpose of preventing or detecting crime, or under any enactment or rule of law or where the course of conduct was reasonable.⁵⁶⁸ The Act imposes both civil⁵⁶⁹ and criminal⁵⁷⁰ sanctions in respect of conduct that amounts to harassment. The Act is a useful remedy where, as has been mentioned, a person annoys or worries another “by putting pressure on them, or by saying or doing unpleasant things to them.”⁵⁷¹

⁵⁶⁶ Chapter 40.

⁵⁶⁷ A S Hornby *Oxford Advanced Learner's Dictionary* (2001) at 541. Cf *Epstein v Epstein* supra where the plaintiff was followed about in public and had her door knocked on every evening for a week. The learned judge (Wessels J) described the acts of the defendants as “a most vexatious nuisance.” However, it has been said that the conduct of the defendants amounted to an invasion of privacy. *McQuoid-Mason* op cit at 87.

⁵⁶⁸ Section 1(3).

⁵⁶⁹ Section 3.

⁵⁷⁰ Section 3(3) – (9). These are later provisions, which came into force on September 1, 1998.

3.2.3.1.2.3a Relevance to Internet Cafes

This Act offers valuable guidance for the protection of electronic mail privacy where bothersome, annoying, or unpleasant mail which puts pressure on another is sent via an Internet café. It will also be applicable where, on Internet café premises, a person worries, annoys or causes distress to an Internet café user by putting pressure on them or doing or saying unpleasant things to them, for instance, where a person verbally threatens another on Internet café premises.

3.2.3.1.2.4 Other Laws Protecting Privacy in the United Kingdom

Other laws with significant privacy components include, the Rehabilitation of Offenders Act,⁵⁷² the Telecommunications Act,⁵⁷³ the Broadcasting Act,⁵⁷⁴ the Theatres Act,⁵⁷⁵ the Copyright, Designs and Patents Act⁵⁷⁶ and the laws protecting rape victims and children in court. These include the Children Act,⁵⁷⁷ the Adoption Act,⁵⁷⁸ the Children and Young

⁵⁷¹ See *Khorsandjian v Bush* supra. See also in *Hunter v Canary Wharf Ltd* supra, Lord Goff at 698, Lord Hoffman at 706. Cf *Epstein v Epstein* supra, where the plaintiff was persistently followed.

⁵⁷² Chapter 53 of 1974.

⁵⁷³ Chapter 12 of 1984.

⁵⁷⁴ Chapter 42 of 1990.

⁵⁷⁵ Chapter 54 of 1968.

⁵⁷⁶ Chapter 48 of 1988.

⁵⁷⁷ Chapter 41 of 1989. In *Re X* [1984] 1 WLR 1422, the High Court granted an injunction prohibiting disclosure of the identity and whereabouts of a child and her mother who had as a juvenile, been sentenced to detention for life for manslaughter and was later released on licence as a ward of the court. The application was made on the ground that the disclosure would threaten the family's new-found peace and stability.

Persons Act,⁵⁷⁹ the Sexual Offences (Amendment) Act,⁵⁸⁰ the Criminal Justice Act,⁵⁸¹ and the Magistrates' Courts Act.⁵⁸² The following are relevant sections protecting privacy in the above listed Acts.

Section 4(1) of the Rehabilitation of Offenders Act makes evidence about a spent conviction inadmissible.⁵⁸³ Under Section 8 of the Act, damages may also be obtained where a person maliciously publishes details of the plaintiff's spent conviction.⁵⁸⁴ Section 43 of the Telecommunications Act makes it an offence to use a public telecommunications system to send grossly offensive, threatening or obscene material.

The Broadcasting Act⁵⁸⁵ contains a provision to the effect that defamatory words, visual images, pictures, gestures and other forms of broadcast on radio or television or any other programme service are actionable as libel.⁵⁸⁶ Similarly, under the Theatres Act,⁵⁸⁷ it is an actionable libel to publish defamatory words in the course of a performance of a play.⁵⁸⁸

⁵⁷⁸ Chapter 36 of 1976.

⁵⁷⁹ Chapter 12 of 1933 (23 & 24 Geo.5).

⁵⁸⁰ Chapter 82 of 1976.

⁵⁸¹ Chapter 33 of 1988.

⁵⁸² Chapter 43 of 1980.

⁵⁸³ Section 4 (1).

⁵⁸⁴ See *Herbage v Pressdram Ltd* [1984] 1 WLR 1160. See also generally Heuston & Buckley op cit at 162.

⁵⁸⁵ Chapter 42 of 1990.

⁵⁸⁶ Section 166.

⁵⁸⁷ Chapter 54 of 1968.

Under the Copyright, Designs and Patents Act,⁵⁸⁹ limited protection for privacy is provided, where a person's proprietary interest in literary⁵⁹⁰ or artistic⁵⁹¹ work has been infringed.⁵⁹² The Act also gives a cause of action for false attribution of authorship.⁵⁹³

Under the Children Act,⁵⁹⁴ proceedings are required to be held in chambers unless the court directs otherwise.⁵⁹⁵

Similarly, section 64 of the Adoption Act⁵⁹⁶ provides that proceedings under that Act should be held in private. Section 49 of the Children and Young Persons Act⁵⁹⁷ restricts reporting of the proceedings of juvenile courts, and section 39 also provides for the obtaining of a court order prohibiting newspaper reports from publishing personal details such as the name, address, school or any detail "calculated to lead to the identification of any child or young person" concerned in proceedings in any case.

⁵⁸⁸ Section 4(1).

⁵⁸⁹ Chapter 48 of 1988.

⁵⁹⁰ Section 3(1).

⁵⁹¹ Section 4(1).

⁵⁹² See generally Heuston & Buckley *op cit* at 38.

⁵⁹³ Sections 83- 84.

⁵⁹⁴ Chapter 41 of 1989.

⁵⁹⁵ Rule 4.16(7) Family Proceedings Rule (1991).

⁵⁹⁶ Chapter 36 of 1976.

⁵⁹⁷ Chapter 12 of 1933 (23 & 24 Geo.5).

Section 4 of the Sexual Offences (Amendment) Act⁵⁹⁸ grants anonymity to victims of rape, and a subsequent amendment⁵⁹⁹ makes it possible to extend the protection of section 4 of the 1976 Act to all cases of sexual offences. The Criminal Justice Act⁶⁰⁰ protects the anonymity of victims in cases involving conspiracy to rape and burglary with intent to rape.⁶⁰¹ Section 69 of the Magistrates' Courts Act⁶⁰² provides that the public is excluded from family proceedings in the magistrates' courts.

The protection guaranteed for privacy in the above statutes is necessarily limited to the subject matter dealt with by the relevant statute, and the specific circumstances provided for and specified in the relevant provisions.

3.2.3.1.2.4a Relevance to Internet Cafes

Although, none of the Acts discussed above focuses directly on the protection of e-mail in Internet cafes, each of the Acts covers a sphere of life that is not excluded from Internet-café related invasions of privacy. For instance, the publication of original poems, songs or other artistic work or composition, disclosure of the names or other protected information relating to victims in rape cases, or the disclosure of information relating to

⁵⁹⁸ Chapter 82 of 1976.

⁵⁹⁹ The Sexual Offences (Amendment) Act; Chapter 31 of 1991.

⁶⁰⁰ Chapter 33 of 1988.

⁶⁰¹ Section 158.

⁶⁰² Chapter 43 of 1980.

adoption proceedings are all possible via e-mail. These statutes provide useful guidelines in similar Internet café related cases.

The above Acts have been cited to demonstrate the utility of specific individual Acts in the protection of privacy⁶⁰³ and they are instructive as examples of details that may be included either in general legislation for the protection of Internet café privacy, or subject-specific Acts as above.

While it is expected that a general Privacy Act or Law will provide a framework and contain general guidelines for the protection of privacy as well as contain several provisions guaranteeing the right to privacy, separate subject-specific privacy legislation afford a degree of detail and depth of legislation on a subject matter that may not be available in a general Act.⁶⁰⁴ When read together with a general Act, subject-specific Acts provide more extensive, thorough and effective protection on any matter and ensure maximal protection in the relevant area.

With specific reference to the protection of electronic mail privacy in Internet cafes in Nigeria, for instance, although a general Privacy Protection Act may provide protection for the infringement of original work processed on Internet café computers, Nigeria also has a Copyright Act⁶⁰⁵ which contains extensive provisions on the protection of artistic

⁶⁰³ Cf below Para 5.

⁶⁰⁴ Cf the 1952 and 1996 U.K. Defamation Acts. (Chapter 66 of 1952 and Chapter 31 of 1996 respectively) Above at Para 3.2.3.1.2.2.

⁶⁰⁵ Cap 68 LFN 1990. See below Chapter 7.

and literary work and as such should also be referred to for protection in cases of copyright infringement.

3. 2. 3. 2 Statutory Protection of Data in the United Kingdom

Prior to 1998, the Data Protection Act of 1984⁶⁰⁶ regulated the collection and use of automated data in the United Kingdom.⁶⁰⁷ The 1984 Act was repealed by the Data Protection Act of 1998,⁶⁰⁸ which came into force on March 1st 2000. The 1998 Act was approved to make the United Kingdom law consistent with the European Union's Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data.⁶⁰⁹

3.2.3.2 1 The European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data⁶¹⁰

In 1981, the Council of Europe issued the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.⁶¹¹ This was an international document formulated specifically to safeguard the right to privacy with regard to the automatic processing of personal data⁶¹² and generally to regulate national data protection

⁶⁰⁶ Chapter 35 of 1984.

⁶⁰⁷ See the Preamble to the Act.

⁶⁰⁸ Chapter 29 of 1998.

⁶⁰⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

standards and to improve and guarantee the free flow of data internationally.⁶¹³ The Convention was followed in 1995 by the Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data.⁶¹⁴

The 1995 European Union Directive contains extensive provisions regulating data practice among its member nations. It provides a general standard that the data protection laws of its member nations should attain,⁶¹⁵ and it prohibits data transfer between its members and other countries that do not provide for “adequate” privacy protection.⁶¹⁶ The EU Directive provides for strong control over the collection and use of personal data among its member nations.

In 2002, the EU adopted a directive which translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.⁶¹⁷ This was followed in March 2006 by a directive on the retention of data generated in connection

⁶¹⁰ Directive 95/46/EC (subsequently referred to as the Directive, the EU Directive, the European Union Data Directive or Directive 95/46/EC).

⁶¹¹ Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Strasbourg 28 January 1981. No 108/1981.

⁶¹² See Chapter 1 Article 1 of the Convention.

⁶¹³ Cf A Roos *The Law of Privacy (Data) Protection: A Comparative and Theoretical Study* (2003) at 152.

⁶¹⁴ Directive 95/46/EC.

⁶¹⁵ Article 6(1).

⁶¹⁶ Article 25. See the Preamble to the Directive.

⁶¹⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

with the provision of publicly available electronic communications services.⁶¹⁸ Directive 2006/24/EC amends Directive 2002/58/EC.

3.2.3.2.1a Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data⁶¹⁹

Mention must also be made here of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.⁶²⁰ The Guidelines preceded the European Union Directive⁶²¹ and have been significantly instrumental in shaping contemporary data protection law.⁶²² The Guidelines were developed by the Committee of Ministers of the Organisation for Economic Co-operation and Development (OECD) against the background of increased international transfer of information and the problems of data violations and misuse.⁶²³

Their purpose was to support member nations in the prevention of human rights violations relating to the storage, disclosure, use or abuse of personal data by

⁶¹⁸ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

⁶¹⁹ (The OECD Guidelines) 1980.

⁶²⁰ Ibid.

⁶²¹ Directive 95/46/EC.

⁶²² Cf Roos op cit at 152-154.

⁶²³ Cf the Preface to the Guidelines. See also Roos op cit at 151ff.

harmonising the national privacy laws of member states, and also to prevent interruptions in international flows of data.⁶²⁴

The OECD Guidelines set out eight principles⁶²⁵ for effective data protection. These have been summarized viz: the principle of limitation of collection, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle and accountability principle.⁶²⁶ It has been suggested⁶²⁷ that the principles should be read as a whole as they are inter-related and a clear or absolute distinction might not exist in the activities and processes involved in complying with the principles.

Although they are not listed or highlighted in the same form in both documents, the OECD data principles are affirmed and reflected in the EU documents.⁶²⁸ This will be seen in the following examination⁶²⁹ of the United Kingdom Data Act⁶³⁰ where the principles are shown to overlap. With reference to the foundation of the data protection

⁶²⁴ Ibid.

⁶²⁵ Part Two sections 7-14 of the Guidelines.

⁶²⁶ See generally Roos op cit at 161-169.

⁶²⁷ Paragraph 50 of the Explanatory Memorandum to the OECD Guidelines.

⁶²⁸ Cf Roos op cit at 152. See also below Paras 3.2.3.2.2.2 ff particularly Para 3.2.3.2.2.5.

⁶²⁹ Paras 3.2.3.2.2.2ff

⁶³⁰ Cap 29 of 1998.

principles, both the OECD and the EU documents⁶³¹ will be referred to concurrently in this work.

3.2.3.2.1.1 General Data Protection Features of the European Union Directive

The European Union Data Directive contains several features and provisions that enhance effective data protection. The Directive covers all manual⁶³² and electronic records.⁶³³ It applies to personal data processed wholly or partly by automatic means as well as personal data processed otherwise than by automatic means, where such data “form part of a filing system or are intended to form part of a filing system”.⁶³⁴ In other words, both computer-stored records and data stored on paper are covered by the provisions of the Directive.

The Directive provides generally that “data capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the subject gives explicit consent”.⁶³⁵ It also specifically forbids the processing of special categories of data except under certain conditions.⁶³⁶ These include data revealing racial or ethnic origin, political opinions, religious beliefs, as well as data concerning health or sex life.⁶³⁷

⁶³¹ Being the latter and more prominent (Cf Roos op cit at 153) of the two documents, particular focus in this work will be on the EU Directive rather than the Convention.

⁶³² Article 2(b).

⁶³³ Article 2(b), (c); Article 3(1); See also P Marett *Intellectual Property Law* (1996) at 150-151.

⁶³⁴ Article 3(1).

⁶³⁵ See the Preamble to the Directive.

The Directive also contains provisions preventing personal data protected under the Directive from losing its protection when transferred to a third country. Where information is protected under the data protection laws of a Member State, unless one of the exceptions set out in Article 26⁶³⁸ is present, such data will enjoy the protection it had in the Member State when transferred to a third country.

The European Union Directive sets out the definitions of certain key terms relating to data protection such as “personal data”,⁶³⁹ “processing”,⁶⁴⁰ “filing system”,⁶⁴¹ “controller”,⁶⁴² and “processor”.⁶⁴³

3.2.3.2.1.2 Data Protection Principles in the Directive

⁶³⁶ Article 8.

⁶³⁷ Article 8(1) & (2).

⁶³⁸ These include consent of the data subject or other lawful justification for such transfer. (Article 26(1) a-f).

⁶³⁹ Article 2(a): Personal data is defined as “any information relating to an identified or identifiable natural person” who is also known as the “data subject”.

⁶⁴⁰ Article 2(b): Processing includes “collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available” and it includes “alignment or combination, blocking, erasure or destruction” either by automatic means or otherwise.

⁶⁴¹ Article 2(c): “Personal data filing system” “Filing system” is defined as “any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis”.

⁶⁴² Article 2(d): “Controller” is defined as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.

⁶⁴³ Article 2(e): “Processor” is “the natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller”.

Several principles of data protection are affirmed under the Directive. These include the right to know where the data originated,⁶⁴⁴ the right to know the identity of data controllers or their representatives,⁶⁴⁵ the purposes for which data is being processed,⁶⁴⁶ the categories of data being processed⁶⁴⁷ as well as the recipients or categories of recipients of data,⁶⁴⁸ the right to withhold permission to use data in some circumstances,⁶⁴⁹ the right to have inaccurate data rectified,⁶⁵⁰ and a right to recourse in the event of unlawful processing.⁶⁵¹ The Directive also provides for the confidentiality of processing.⁶⁵²

3.2.3.2.1.3 Liability under the Directive

Article 4 of the Directive makes a controller subject to the law of a Member State in which it has an establishment and undertakes processing.⁶⁵³ It also makes a controller

⁶⁴⁴ Article 12 (1).

⁶⁴⁵ Article 10(a), Article 11(a).

⁶⁴⁶ Article 10(b), Article 11(b).

⁶⁴⁷ Article 11(c).

⁶⁴⁸ Article 10(c), Article 11(c).

⁶⁴⁹ Article 14.

⁶⁵⁰ Article 12(2).

⁶⁵¹ Article 22, Article 23.

⁶⁵² Article 16. This provision prohibits the processing of data by data controllers, processors and others acting under the authority of the processor except under instruction from the controller or authority of the law.

⁶⁵³ Article 4 (1)(a).

from outside the European Union who makes use of data processing equipment within the European Union other than for the sole purpose of data transit data through the Member State, subject to the law of that Member State.⁶⁵⁴ In essence, on-line traders dealing with customers within the European Union must follow European Union regulatory principles since they process information via customers' computers.⁶⁵⁵

The provisions in the Directive are not directly enforceable by citizens as the Directive is addressed to the member states, which are required to incorporate and reflect the Directive principles in their national law.⁶⁵⁶ Thus, the protection for privacy and data provided for by the Directive is dependent on, and directly enforceable only through the national laws of the country in which the infringement of privacy occurred.

3.2.3.2.1.4 Relevance to Internet Cafes

Several aspects of the EU Directive will provide valuable guidelines in enacting legislation for the protection of electronic mail and data processed in Internet Cafes in Nigeria. The Preamble to the Directive sets out a fundamental aspect of data or privacy

⁶⁵⁴ Article 4(1)(c).

⁶⁵⁵ The Directive was written prior to the Internet Revolution and it has been observed that there is very little jurisprudence on this provision. Cf Wikipedia Contributors *Directive 95/46/EC on the protection of personal data* http://en.wikipedia.org/wiki/directive_95/46/EC_on_the_protection_of_personal_data. Accessed February 9, 2007.

⁶⁵⁶ See the Directive Recitals generally and at Paras 68 and 69. See also Articles 4 and 10 of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of personal Data. Cf Roos op cit at 155. See also Wikipedia Contributors *Directive 95/46/EC on the protection of personal data* http://en.wikipedia.org/wiki/directive_95/46/EC_on_the_protection_of_personal_data Accessed February 9, 2007.

protection, which is the prohibition of data capable of infringing on personal liberty, autonomy, self-determination or the right to choose.

The Directive further provides certain aspects or spheres of life in respect of which there ought to be freedom from intrusion.⁶⁵⁷ These provisions are instructive not only for the protection of electronic mail or Internet café related privacy invasion cases, but for general data protection.

Further to this, the data protection principles detailed in the Directive⁶⁵⁸ represent general data protection standards applicable for the protection of any processed information. They have been identified as the foundational principles of data protection.⁶⁵⁹ These principles and their relevance for the protection of electronic mail and other data processed in Internet cafes will be discussed in greater detail in the examination of the 1998 Data Protection Act.⁶⁶⁰

Lastly, the definition, in the Directive, of key terminology provides a clear and consistent reference point. The above features are all elements to be included in any law for the

⁶⁵⁷ Article 8. Cf J Neethling, J M Potgieter, P J Visser *Law of Delict* (2006) at 335; D McQuoid-Mason "Privacy" in M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz, S Woolman (eds) *Constitutional Law of South Africa* (2004) at 38-1. See also Roos op cit at 555 & 556.

⁶⁵⁸ Articles 10, 11, 12, 14, 22, 23; See above Para 3.2.3.2.1.1.

⁶⁵⁹ Cf Roos op cit at 1 ff.

⁶⁶⁰ See below Para 3.2.3.2.2 .

protection of electronic mail and other information processed in Internet cafes, and will form a solid foundation for a Nigerian data protection law.

3.2.3.2.2 The 1998 Data Protection Act⁶⁶¹

The major difference between the 1984 Act⁶⁶² and the 1998 Act⁶⁶³ in the United Kingdom is that while the former regulated the use of only automated files about individuals, the 1998 Act applies to paper-based records as well as automated or electronic records,⁶⁶⁴ in line with the EU Data Protection Directive.⁶⁶⁵ However, many of the basic provisions of the 1984 Act and the 1998 Act are similar.

3.2.3.2.2.1 Definitions

The 1998 Act defines such terms as “data”, “personal data”, “data subject”, “data controller”, “data processor”, and “processing”, among others⁶⁶⁶ as set out below.

3.2.3.2.2.1.1 Data

⁶⁶¹ Cap 29 of 1998.

⁶⁶² Cap 35 of 1984.

⁶⁶³ Cap 29 of 1998.

⁶⁶⁴ Section 1(1).

⁶⁶⁵ Article 3; See also Para 27 of the recitals of Directive 95/46/EC.

⁶⁶⁶ See generally Part I Section 1.

In the Act, "*data*" is defined as

“information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68”

3.2.3.2.2.1.1a Annotation

This definition of data covers manually recorded as well as automatically processed information and applies whether the information is in the process of being recorded, or already exists in recorded form or it is being processed. In Nigeria, a substantial amount of records exists in handwritten or typed format. By the definition above, such information, including information contained in a temporary form, for instance a jotting on a note-pad will be regarded as data.

Information relating to curriculum vitae, personal data, family information, business and other information processed by means of a computer will also qualify as data under the Act. Thus, information processed in Internet cafes will ordinarily qualify as data.

3.2.3.2.2.1.2 Personal Data

“*Personal data*” is defined in the Act as “data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.”⁶⁶⁷ The definition of personal data in the Act includes “any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.”⁶⁶⁸

3.2.3.2.2.1.2a Annotation

The definition of personal data to include facts as well as opinion and intentions relating to an individual reflects the various forms in which data exists and may affect individuals today. This definition of personal data guarantees a wide range of protection for individuals in respect of the varieties of information held about them. It is noteworthy that data must relate to a living person. This means that action cannot be brought on behalf of a deceased person for instance to straighten records⁶⁶⁹

From this definition, it can be affirmed that where a person processes information relating to him or herself, or any other living person in an Internet café, if the person to whom the information relates can be identified, the data processed qualifies as personal data. Thus,

⁶⁶⁷ Section 1(a) & (b).

⁶⁶⁸ *Ibid.*

⁶⁶⁹ Cf the German *Mephisto* case where a son successfully brought action with regard to information published about his deceased father. Cf below Chapter 5.

such information as curriculum vitae and information contained in certain personal and family letters processed in Internet cafes qualify as personal data.

3.2.3.2.2.1.3 Data Subject

“*Data subject*”, according to the Act, “is an individual who is the subject of personal data.”⁶⁷⁰

3.2.3.2.2.1.3a Annotation

With regard to Internet cafes, it may be deduced from the preceding that it is not necessary to personally process information in an Internet café to qualify as a data subject. It will suffice if information relating to the individual, from which, that individual may be identified, is processed. This definition allows third parties about whom personal information (data) is processed in Internet cafés by others to be regarded as data subjects and as such, to exercise the rights accruing to data subjects under the Act.

For instance, where personal information (or data) concerning family members is processed by another family member in an Internet café, even where the other family members are not present at the Internet café at the time of the processing, they may qualify as data subjects under the Act.

3.2.3.2.2.1.4 Data Controller

The Act defines “*data controller*”, as “a person who (either alone or jointly or in common with other persons) determines the purposes for which and manner in which any personal data are, or are to be, processed.”⁶⁷¹ This includes persons required by law or under regulation to process personal data for specific purposes or pursuant to certain enactments.⁶⁷²

3.2.3.2.2.1.4a Annotation

Internet café owners and their staff determine the manner in which information is organised and stored in their computers. They hold personal data, allow clients to keep a code or password that gives access to their accounts and files, in which information is stored, and in some cases they know the customers’ passwords. Internet café operators also keep custody of computers that store messages and are able to access client files if left open.

By electing to retain, or, not to delete certain information processed on their computers, they also determine what information is retained and the purposes for which such information is held. In addition they are in a position to determine the manner in which and purpose for which data in their possession may be obtained, retrieved, consulted or

⁶⁷⁰ Section 1(1).

⁶⁷¹ Ibid.

disclosed. As such, Internet café workers are data controllers within the meaning of the United Kingdom Data Act.

3.2.3.2.2.1.5 Processing

“*Processing*”, with regard to information or data in the Act, means “obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.”⁶⁷³ This includes organisation, adaptation, alteration, retrieval, consultation, use or disclosure.⁶⁷⁴

3.2.3.2.2.1.5a Annotation

The definition of processing given by the Act is wide and generally covers the categories of interests protected by the right to privacy as identified by Prosser (i.e. intrusions, public disclosure, appropriation and false light).⁶⁷⁵

Internet café owners and employees carry out many of the functions that qualify as processing. They obtain, hold, record, organise, adapt and are able to alter, consult and retrieve information contained in computers in their custody.⁶⁷⁶

⁶⁷² Section 1 subsection 4.

⁶⁷³ Ibid.

⁶⁷⁴ Section 1(1)(a) to (d).

⁶⁷⁵ See above Para 1.1.

3.2.3.2.2.2 Rights of Data Subjects under the Act

Part II of the Act deals with the rights of data subjects and provides specifically for the right of access to personal data.⁶⁷⁷ Under this section, a data subject is entitled to be informed by any data controller whether personal data concerning him or her is being processed by, or on behalf of that data controller.⁶⁷⁸ The data subject is further entitled to a description of the data, the purpose of processing such data, and the recipient or classes of recipients to whom the data has been, or may be disclosed.⁶⁷⁹

The provisions of section 7 (1) address one of the major privacy concerns arising from the technology revolution, which is the fact that information can be acquired without the knowledge and, or, consent of the individual.⁶⁸⁰ There can be no exercise or enjoyment of privacy or data protection where there is no knowledge by the subject that personal data regarding them is being processed. Thus, knowledge of the fact of processing is a prerequisite for the exercise of privacy and data protection rights.

In addition, where the processing by automatic means of data relating to an individual for the purpose of evaluating matters relating to him or her, (e.g. at work or creditworthiness), has constituted, or is likely to constitute, the sole basis for a decision

⁶⁷⁶ Cf above Para 3.2.3.2.2.1.4a.

⁶⁷⁷ Section 7.

⁶⁷⁸ Section 7(1) a.

⁶⁷⁹ Section 7(1) b.

⁶⁸⁰ Cf above Para 1.2.

defined by the Act, as “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.”⁶⁸⁷

These provisions allow data subjects to determine and restrict the use, (including access to, and disclosure or publication), of information regarding themselves, thereby giving them a measure of control over such information.

Section 14 of the Data Protection Act provides that where processed data is inaccurate, the court may order the data controller to rectify, block, erase or destroy the data as well as any other processed data which contains an expression of opinion that appears to the court to be inaccurate.⁶⁸⁸ Under this section, the Act also provides that where it is reasonably practicable, the court may order the data controller to notify third parties to whom data have been disclosed, of rectification, blocking, erasure or destruction of data.⁶⁸⁹ This provision purports to prevent the disclosure, publication or usage in any way, of inaccurate information or data, and in this way, protects the data subject’s privacy.

The OECD openness principle⁶⁹⁰ is upheld in the provisions requiring the data subject to be informed of the fact of processing⁶⁹¹ while the provisions relating to the data subject’s

⁶⁸⁷ Section 11(3).

⁶⁸⁸ Section 14.

⁶⁸⁹ Section 14(5).

⁶⁹⁰ Cf above Para 3.2.3.2.1.2.

right of access,⁶⁹² right to reasons⁶⁹³ and right to challenge⁶⁹⁴ espouse the individual participation principle.

3.2.3.2.2.2a Relevance to Internet Cafes

Generally, the provisions contained in Part II of the Act empower a data subject to exercise control⁶⁹⁵ over information and also provide checks and limitations on the power of data processing authorities in the gathering, use and dissemination of information. These provisions, and in particular, the principles they represent, are relevant for the protection of privacy in Internet cafes and they will be examined in greater detail below.⁶⁹⁶

3.2.3.2.2.3 The Data Protection Commissioner

⁶⁹¹ Section 7(1)(a) & (b) DPA. Cf Roos op cit at 165.

⁶⁹² Sections 7(1) & 7(2). Cf Roos op cit at 167.

⁶⁹³ Section 7(1)d. Cf Roos op cit at 167.

⁶⁹⁴ Sections 10, 11, & 14. Cf Roos op cit at 168.

⁶⁹⁵ Cf I J Sloan *Law of Privacy Rights in a Technological Society* (1986) at 13 (above Para 1.1) See also O M Ruebhausen & O G Brim "Privacy and Behavioural Research" (1965) 65 *Columbia Law Report* at 1185. Cf C Fried "Privacy" (1968) 77 *Yale Law Journal* 483 above Para 1.1

⁶⁹⁶ At Para 3.2.3.2.2.5.

The Act makes provision for a Data Protection Commissioner,⁶⁹⁷ whose duty includes among others, promoting the following of good practices by data controllers⁶⁹⁸ and assisting individuals in proceedings relating to data under the Act.⁶⁹⁹ A duty of confidentiality is imposed on the Commissioner and any members of the Commissioner's staff, or an agent.

They are prohibited from disclosing information relating to an identified or identifiable individual or business, which was obtained by, or furnished to the Commissioner under, or for the purposes of the Act, and not previously available to, or known by, the public from other sources except under certain circumstances without lawful authority.⁷⁰⁰ This is in line with the Common Law duty of confidence arising out of professional relationships.⁷⁰¹

The Act makes provision for specific matters and duties to be performed by the Data Commissioner.⁷⁰² However many of the provisions that set out the general duties and functions of the Commissioner⁷⁰³ also permit considerable latitude and discretion in the

⁶⁹⁷ Section 6.

⁶⁹⁸ Section 51.

⁶⁹⁹ Section 53.

⁷⁰⁰ Section 59; This section effectively places responsibility on all who process data to maintain confidentiality.

⁷⁰¹ Cf above Para 3.2.2.1.1.2.

⁷⁰² Section 19, which provides for register of notifications, section 20 on the duty to notify changes, and section 22 on preliminary assessment by the Commissioner.

performance of these duties. For instance, Section 45 (1) of the Act provides in part as follows,

“Where... it appears to the Commissioner... that any personal data are not being processed only for the special purposes, or ...with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller, [the Commissioner] may make a determination in writing to that effect...”

This means that the final determination as to whether or not personal data are being processed in accordance with the Act’s requirements on purpose specification lies with the Commissioner. Further to this, according to the wording of Section 45(1) the Commissioner is not compelled to take further action in respect of any perceived non-compliance. The use of the word “may”, instead of “shall” merely assents to the Commissioner’s authority or permission to carry out the act, and may be read as implying uncertainty, doubt or the absence of obligation.⁷⁰⁴

In any case, the wording of Section 45 does not impose an obligation to act. In effect, where there has been a violation of the Act relating to compliance with the provisions on

⁷⁰³ See generally, Part VI Section 51 which provides that the Commissioner shall “arrange for the dissemination *in such form and manner as he considers appropriate* of such information as *it may appear to him expedient* to give to the public about the operation of this Act, about good practice, and about other matters within the scope of his functions under this Act”

⁷⁰⁴ Cf the use of the wording “must” and “shall” in Sections 17 and 18 prohibiting processing without registration and notification by Data Controllers. See also Dorling Kindersley, *The Illustrated Oxford Dictionary* (2003) at 506.

special purposes, the data subject must rely on the Commissioner's discretion in taking steps to rectify the situation. Where the Commissioner does not take any steps, he or she cannot be compelled to take action.

It must also be noted that there are exceptions to the general provisions of the Act, and that there may be circumstances under which the protection afforded by the Act may be denied an individual.⁷⁰⁵

3.2.3.2.2.3a Relevance to Internet Cafes

There is no Data Protection Act or Data Commissioner in place in Nigeria. The Computer Security and Critical Information Infrastructure Protection Bill⁷⁰⁶ contains provisions for the protection of computer processed information⁷⁰⁷ but it does not provide for any officer to administer, oversee or ensure compliance with the Bill, therefore it affords no basis for comparison. More importantly, the Bill is yet to come into operation thus it cannot be relied on for the present purpose.

⁷⁰⁵ These include reasons of national security (Section 28), crime and taxation (Section 29), and health, education and social work (Section 30). This is in line with the principle that no right is absolute and that the individual's interest has to be balanced against other interests in deciding whether or not to uphold a claim to privacy. (Cf above Para 1.1).

⁷⁰⁶ 2005.

⁷⁰⁷ See generally the Preamble to, and Parts I & II of the Bill.

It will be assessed below⁷⁰⁸ whether data protection legislation is needed in Nigeria and, if needed, whether there ought to be provision for an administrative officer similar to the United Kingdom Data Protection Commissioner to oversee the Nigerian Act.

3.2.3.2.2.4 Data Controllers

The United Kingdom Data Act also contains provisions regulating data controllers.⁷⁰⁹ Section 16 provides that data controllers must be duly registered with the Commissioner. This section specifies that data controllers must give certain information pursuant to registration. This information includes personal details such as the names and addresses of the controllers,⁷¹⁰ (and their representatives, where applicable),⁷¹¹ the category or categories of data subjects to which they relate,⁷¹² a description of the purpose or purposes for which the data is to be processed,⁷¹³ and the recipient or recipients to which the data controllers may wish to disclose data or information.⁷¹⁴

Section 17 prohibits a data controller from processing personal data where such data controller is not registered with the Commissioner. The Act also requires that data

⁷⁰⁸ Chapter 8 Para 8.2.

⁷⁰⁹ Part III.

⁷¹⁰ Section 16(1)(a).

⁷¹¹ Section 16(1)(b).

⁷¹² Section 16(1)(c).

⁷¹³ Section 16(1)(d).

⁷¹⁴ Section 16(1)(e).

controllers specify general measures to be taken by them for the purpose of complying with the Seventh data protection principle,⁷¹⁵ which provides that appropriate technical organisational measures must be taken against unauthorised or unlawful processing of personal data as well as accidental loss, destruction or damage.⁷¹⁶

Such regulation of the operations of data controllers serves as a check on their powers, constraining them to remain within the limits specified in processing information. It serves to ensure that they exercise due care and responsibility in the discharge of their duties and that they comply with the provisions of the Act, adhere to the Data Protection Principles,⁷¹⁷ and particularly, the Seventh principle.⁷¹⁸

The Seventh principle correlates to the OECD Security Safeguards principle.⁷¹⁹ Generally, the provisions regulating the practices of data controllers and prescribing procedures and to be followed by them are in line with the OECD limitation of collection principle, data quality principle, purpose specification, use limitation, openness principle and accountability principle.⁷²⁰

⁷¹⁵ Section 18(2)(b).

⁷¹⁶ Schedule 1.

⁷¹⁷ Schedule 1 to the Act; See above Para 3.2.2.2.1.

⁷¹⁸ The Seventh principle provides for appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data as well as accidental loss, destruction of or damage to data. (Schedule 1 Para 7).

⁷¹⁹ Cf above Para 3.2.3.2.1.2.

⁷²⁰ Part II. Cf above Para 3.2.3.2.2.2.

3.2.3.2.2.4a Relevance to Internet Cafes

As established above,⁷²¹ Internet café owners and operators determine the purposes for which and manner in which personal data are processed and are data controllers. The provisions relating to data controllers are thus relevant for regulating the operations of Internet café owners affecting the privacy of their customers and are generally applicable with regard to any information processed on the Internet café premises or with Internet café equipment.

Although there are other laws that provide for privacy protection in Nigeria, there is a lacuna in this area of the law. The Nigerian Constitution⁷²² contains provisions for the protection of privacy,⁷²³ but these are general provisions that have not received much judicial attention or interpretation and are not detailed regarding information gathering, storage and other practices of data controllers.

In addition to the constitutional guarantee of privacy, the Computer Security and Critical Information Infrastructure Protection Bill⁷²⁴ contains relevant provisions for the regulation of privacy and data in Internet cafés. These provisions have however been

⁷²¹ Cf above Para 3.2.3.2.2.1.4.

⁷²² 1999 Constitution FRN.

⁷²³ Cf below Chapter 7.

⁷²⁴ 2005. Cf below Para 7.2.2.2.1.

criticized⁷²⁵ and the Bill shown to be deficient in protecting privacy.⁷²⁶ Other laws in Nigeria with privacy content⁷²⁷ do not regulate the practices of data controllers. There is undoubtedly a need for provisions regulating the operations of data processors and controllers in Nigeria.

The requirement for registration, specification of purpose and other necessary or desirable requirements to be included in a Nigerian law regulating the operations of data controllers will be discussed below.⁷²⁸

3.2.3.2.2.5 Eight Data Protection Principles

The rights and duties provided for in the United Kingdom Data Protection Act, including some of those discussed above have been distilled into eight principles of data protection specifically set out in the 1998 Data Act.⁷²⁹ These principles are included in different variations in other data protection laws⁷³⁰ and Guidelines⁷³¹ and they have been identified, in essence as basic principles of data protection.⁷³²

⁷²⁵ See Eijeagbon Ohigheoga "Nigeria: New Wire Tapping, Cyber Crimes Bill in Nigeria" <http://lists.jammed.com/ISN/2006/10/0090.htm> Accessed February 2007.

⁷²⁶ Ibid.

⁷²⁷ Cf below Para 7.2.2.2.

⁷²⁸ Para 3.2.3.2.2.5 and Chapter 9.

⁷²⁹ Part I Schedule 1, United Kingdom Data Protection Act 1998.

⁷³⁰ The repealed 1984 U.K. Data Protection Act, the United States of America Privacy Act, the German Privacy Act, the proposed South African Data Act and the Canadian Privacy Act among others. See also Roos op cit at 480.

They include fair and lawful processing of data,⁷³³ specifying the purpose for which data is obtained, prohibition of processing incompatible with the specified purpose,⁷³⁴ personal data being adequate, relevant,⁷³⁵ accurate and up-to-date where necessary,⁷³⁶ among others as set out below.

“1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2⁷³⁷ is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3⁷³⁸ is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

⁷³¹ For example, the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. 1980. Cf above Para 3.2.3.2.1.2.

⁷³² Cf Neethling *Persoonlikheidsreg* (1985) at 336-337 as cited in Roos op cit at 650. See also Bainbridge *Data Protection Law* 66 as cited in Roos op cit at 280. See generally Roos op cit in chapters 3, 4, 8 and 9 for an extensive discussion on the data protection principles.

⁷³³ Principle 1.

⁷³⁴ Principle 2.

⁷³⁵ Principle 3.

⁷³⁶ Principle 4.

⁷³⁷ Schedule 2 specifies conditions precedent for the processing of personal data with reference to the First Principle. These include consent by the data subject for such processing and a list of specific conditions rendering such processing necessary.

⁷³⁸ Schedule 3 sets out conditions for the processing of Sensitive Personal Data for the purpose of the First Principle. These include explicit consent by the data subject for such processing and a list of specific conditions rendering processing necessary.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

3.2.3.2.2.5a Annotation on the Data Protection Principles

(i) First Principle: Fair and Lawful Processing

The first part of this provision is a requirement for fair and lawful processing of data. The terms “fair” and “lawful” are not defined in the Act. However, in line with the first rule of statutory construction,⁷³⁹ it may be asserted that processing will be “fair” where it is

equitable, just, honest and/or in accordance with the rules.⁷⁴⁰ In this regard, the Act contains specific and detailed provisions⁷⁴¹ stipulating requirements to be met in order for processing under the First principle to be regarded as fair. This includes the requirement that regard must be had to the method of obtaining the information⁷⁴² and the source/s of the information.⁷⁴³ The Act also provides for specified information⁷⁴⁴ to be supplied to the data subject pursuant to the obtaining of data from them.⁷⁴⁵ These requirements espouse the OECD Openness Principle.

As for lawful processing, again following the first rule of statutory construction, data will be processed “lawfully” where processing conforms with, is permitted by, and/or does not constitute a breach of (any relevant) law.⁷⁴⁶ Since Schedules 2 and 3 of the Act contain conditions to be fulfilled for the processing of data under the First principle, it

⁷³⁹ Also known as the “plain meaning” rule. This rule dictates that statutes are to be interpreted in accordance with the plain, ordinary and literal meaning of the language of the statute unless the result of such interpretation would be cruel or absurd. It is often the first rule to be applied in construing statutes. See *Muller v. BP Exploration (Alaska) Inc.*, (1996) 923 P.2d 783, 787-88; *Connecticut Nat'l Bank v. Germain*, (1992) 112 S.Ct. 1146, 1149. Cf the Golden rule in the United Kingdom; *Grey v. Pearson* (1857) 6 HL CAS 61; *Becke v Smith* (1836) 2 M&W 195.

⁷⁴⁰ Ibid.

⁷⁴¹ Schedule 1 Part II.

⁷⁴² Schedule 1 Part II Section 1(1); This includes the determination as to whether the person from whom the data is obtained is misled or deceived as to the purpose for which the data is to be processed.

⁷⁴³ Schedule 1 Part II Section 1(2); To qualify as having been processed fairly, data must be supplied by (a) person/s who is/are either authorised or required by law to supply such information.

⁷⁴⁴ Schedule 1 Part II Section 2(3); This includes such information as the identity of the data controller or of his/her representatives where applicable, the purpose/s for which the data is to be processed and other necessary information to enhance fairness towards the data subject in the processing of such information.

⁷⁴⁵ Schedule 1 Part II Section 2.

⁷⁴⁶ Cf D Kindersley *The Illustrated Oxford Dictionary* (2003).

may be asserted that, at the most basic level, compliance with the provisions of these Schedules is required for lawful processing.

Schedule 2 sets out the conditions relevant for the processing of data under the First principle. The Schedule provides for the obtaining of the consent of the data subject prior to processing.⁷⁴⁷ It also provides that such processing must be necessary.⁷⁴⁸ Processing will be lawful if either the consent of the data subject has been obtained, or the processing is necessary for a specific purpose stated in the Act. In this regard, specific instances in which processing will be deemed necessary are set out in the Schedule.

These include: the performance of a contract or request for processing by a data subject for the purpose of entering into a contract,⁷⁴⁹ compliance with a legal obligation to which the data controller is subject,⁷⁵⁰ the protection of vital interests of the data subject,⁷⁵¹ the administration of justice⁷⁵² and for legitimate ends or interests pursued by the data controller or by a third party or parties to whom the data are disclosed except where processing is prejudicial to the rights or interests of the data subject.⁷⁵³

⁷⁴⁷ Schedule 2(1).

⁷⁴⁸ Schedule 2(2) – (6).

⁷⁴⁹ Schedule 2(2).

⁷⁵⁰ Except for obligations imposed by contract Schedule 2(3).

⁷⁵¹ Schedule 2(4).

⁷⁵² Schedule 2(5).

⁷⁵³ Schedule 2(6).

Schedule 3 sets out the conditions for the processing of sensitive personal data. Sensitive personal data is defined in terms of Section 2 of the Act as information relating to-

- (a) one's racial or ethnic origin,
- (b) political opinions,
- (c) religious beliefs or other beliefs of a similar nature,
- (d) whether one is a member of a trade union,
- (e) one's physical or mental health or condition,
- (f) one's sexual life,
- (g) the commission or alleged commission by the data subject of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

As in Schedule 2, the first condition listed for lawful and fair processing is the obtaining of consent from the data subject.⁷⁵⁴ It must be noted that explicit consent is required in the case of sensitive personal information.⁷⁵⁵ Furthermore, Schedule 3 provides a more detailed list than Schedule 2 of cases in which processing may be carried out without the consent of the data subject. These include cases where the processing is necessary:

⁷⁵⁴ Schedule 3(1). Note that

⁷⁵⁵ Ibid.

(a) for the exercise or performance of a right or obligation conferred or imposed by law on the data controller in connection with employment.⁷⁵⁶

(b) to protect the vital interests of the data subject or another person, in cases where-

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject.⁷⁵⁷

(c) for the protection of the vital interests of another, not being the data subject, in a case where consent by or on behalf of the data subject has been unreasonably withheld.⁷⁵⁸

(d) in connection with any legal proceedings, for the purpose of obtaining legal advice, or for the purposes of establishing, exercising or defending legal rights.⁷⁵⁹

(e) for the administration of justice, for the exercise of any functions conferred on any person by or under an enactment, or for the exercise of any governmental function.⁷⁶⁰

(f) for medical purposes⁷⁶¹ and is undertaken by a health professional, or a person who could be deemed to owe a duty of confidentiality equivalent to that of a health professional.⁷⁶²

⁷⁵⁶ Schedule 3(2).

⁷⁵⁷ Schedule 3(3)(a).

⁷⁵⁸ Schedule 3(3)(b).

⁷⁵⁹ Schedule 3(6).

⁷⁶⁰ Schedule 3(7).

⁷⁶¹ This is defined in Schedule 3(7)(2) as including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

⁷⁶² Schedule 3(8).

Schedule 3 also allows for the processing of sensitive personal data relating to racial or ethnic origin where such processing is:

- (i) carried out with appropriate safeguards for the rights and freedoms of data subjects and
- (ii) necessary for the purpose of identifying or reviewing equal opportunity practice or treatment between persons of different racial or ethnic origins, with a view to maintaining and or promoting equality.

Under Schedule 3, personal data may also be processed by certain non-profit organisations or associations under circumstances specified in the Schedule,⁷⁶³ where the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject⁷⁶⁴ and in circumstances specified in an Order made by the Secretary of State⁷⁶⁵

In both Schedules 2 and 3, the first requirement for processing is the consent of the data subject. It is arguable that compliance with this requirement alone will successfully eliminate most data invasion and/or misuse problems.

However, it is not always feasible or practicable to obtain such consent. For instance, where data is needed to attend to the data subject's health problem and the data subject is

⁷⁶³ Schedule 3(4).

⁷⁶⁴ Schedule 3(5).

⁷⁶⁵ Schedules 10; 7(2) and 9(2).

not medically capable of making a sound decision in his/her own interest regarding the release of such data. In such a case, data may be obtained or retrieved by the data subject's doctor or health care provider pursuant to Schedule 3 (8). Processing will be regarded as lawful if at least one of the conditions in the relevant schedule as well as one of the grounds enumerated in schedule 2 is present.

While it will be impracticable to provide a complete and exhaustive list of instances where processing without the consent of the data subject will be necessary, Schedules 2 and 3 demonstrate an attempt to provide classes of interests that will be recognised in such cases. These may be loosely identified as: the data subject's interest, state interest and interests of other affected third parties. Here, the recognition and balancing of individual rights against the rights of others, and the protection of public and state interests⁷⁶⁶ are underlined.

In effect, in the determination of the question whether processing is fair and lawful, specific standards provided for in the Act are utilised. The provisions clarifying "fair" and "lawful" in the Act must be highlighted for their function in eliminating arbitrariness and enhancing consistency, equality and equity in the interpretation and application of the First principle. The conditions specified for meeting the fairness requirement of the First principle will be in line with the requirements of the OECD Purpose Specification and Openness principles.

⁷⁶⁶ Cf above at 6 & 7.

(ii) Second Principle: Specification of Purpose

The Second principle requires that data controllers specify the purpose for which processing will be done and remain within the limit specified. In effect, data collection cannot be arbitrary; there must be an identified rationale, objective or aim for such collection and/or processing, which must be specified. The essence of this principle is to regulate and constrain data collection, use and general processing within set identifiable limits relevant to the objective or rationale.

The Act provides that notice of the purpose/s for the obtaining of data may be given either directly to the data subject by the data controller⁷⁶⁷ or in a notification to the Commissioner.⁷⁶⁸ It further provides that in determining whether disclosure of data is compatible with the purpose/s for which it is obtained, the purpose/s for which the personal data is intended to be processed by the person to whom it is disclosed must be considered.⁷⁶⁹ The Second principle is parallel to the OECD Purpose Specification and in essence, complies with the OECD Collection Limitation and Use Limitation principles.

(iii) Third Principle: Data Adequacy and Relevance

The Third principle lays out general parameters or standards to which processing must conform. It follows on, and may be regarded as an extension of, the Second principle.

⁷⁶⁷ Schedule 1 Part II Section 5(a).

⁷⁶⁸ Schedule 1 Part II Section 5(b).

The Second and Third principle provide in effect that, not only must processing be done within specified limits in accordance with (a) given purpose(s), processing must also, in relation to the specified purpose be sufficient, proportionate, warranted, necessary, and related.⁷⁷⁰ The third principle is in line with the OECD Collection Limitation and Use Limitation principles.

(iv) Fourth Principle: Data Accuracy

Accuracy is synonymous with correctness, lack of errors, preciseness, exactness and truth⁷⁷¹ therefore data accuracy is a call for information to be correct, precise, exact, and true. This is essential for the avoidance of misrepresentations and crucial in decision-making for arrival at sound conclusions. The Act provides for certain circumstances in which inaccuracies will not be regarded as contravention of the Fourth principle.⁷⁷²

On the basis of the second half of the Fourth principle, information may be updated to reflect the true or correct position if the data subject's circumstances have changed. However, by virtue of the same provision, there is also a restriction imposed on further

⁷⁶⁹ Schedule 1 Part II Section 6.

⁷⁷⁰ Cf The Online Thesaurus (Microsoft Office Word 2003).

⁷⁷¹ Cf the Online Thesaurus op cit. See also Dorling Kindersley, *The Illustrated Oxford Dictionary* (2003 ed) at 20.

⁷⁷² Schedule 1 Part II Section 7. These include situations where, with regard to information is obtained from the data subject or a third party, is accurately recorded a data controller has taken reasonable steps to ensure the accuracy of data with regard to the purpose/s for which it is obtained (Section 7(a)) or, where it is refelcted in the data that the data controller has been notified by the data subject of his/her opinion that the data is incorrect. (Section 7(b)).

processing or update of data where such update is not necessary. The Fourth principle demonstrates an attempt to strike a delicate balance between a possible need for recurrent data collection to ensure accuracy, and the conflicting need to restrict or limit data collection in order to protect individual privacy.

The Fourth principle is consistent in essence with the OECD Collection Use and Limitation Use principles.

(v) Fifth Principle: Storage Limitation

The Fifth Principle provides for the timely disposal or erasure of data where it is no longer needed or required for the original purpose for which it was obtained. This eliminates the threat of access or any other potential form of misuse to such data indefinitely or beyond such time. In providing that data should not be stored beyond the original purpose for its collection, the Fifth principle is in line with the Use Limitation principle of the OECD.

(vi) Sixth Principle: Recognition of Data Subjects' Rights

The Sixth principle provides that processing shall be done in accordance with the rights of data subjects under the Act. These are contained in Part II of the Act.⁷⁷³ By placing responsibility on data controllers to comply with the Act regarding provisions on the

⁷⁷³ Cf above Para 3.2.3.2.2.2.

rights of data subjects, the Sixth principle affirms the OECD Accountability principle which requires data controllers to be accountable for complying with measures that give effect to the OECD principles.⁷⁷⁴ The Act provides for the circumstances under which it will be deemed that there has been a contravention of the Sixth principle.⁷⁷⁵

(vii) Seventh Principle: Precautionary Safety Measures

The Seventh principle calls for precautionary measures for the prevention of unauthorised or unlawful processing of personal data as well as against accidental loss or destruction of, or damage to, personal data. Data controllers must take necessary and proper technological, mechanical, professional, procedural as well as managerial steps in this regard. The Seventh principle places responsibility on data controllers for third party interference with data in their custody. It promotes the theory of prevention as opposed to the remedy or compensation of (data infringement) wrongs. The Seventh principle correlates to the OECD Security Safeguards principle and is in line with the Accountability principle.

(viii) Eighth Principle: International Data Transfer

The Eighth Principle prohibits the transfer of personal data to any country or territory outside the European Economic Area unless that country or territory ensures a

⁷⁷⁴ Cf Roos op cit at 168.

satisfactory or acceptable level of protection for the rights of data subjects regarding the processing of personal data. This effectively guarantees inter-nationally coordinated, equal and consistent data protection for data subjects. It also provides further incentive to other countries to ensure that similar standards are set in their Data protection legislation.

A set of factors are enumerated in the Act⁷⁷⁶ for consideration in determining whether or not an adequate level of protection exists in any case. Schedule 4 of the Act however makes provision for cases where the Eighth Principle will not apply.⁷⁷⁷ The Eighth Principle aims to address one of the major Council of Europe concerns leading to the establishment of the OECD Guidelines.⁷⁷⁸

Although the principles discussed above are each different, it may be said that they are interrelated⁷⁷⁹ in varied degrees and singular in focus and purpose. Accordingly, it is

⁷⁷⁵ Schedule 1 Part II Section 8; which provides in essence that failure to comply with specified procedure in Section 7, 10, 11 or 12 of the Act will constitute a contravention of the Sixth principle.

⁷⁷⁶ Schedule 1 Part II Section 13. These include:

- (a) the nature of the personal data,
- (b) the country or territory of origin of the information contained in the data,
- (c) the country or territory of final destination of that information,
- (d) the purposes for which and period during which the data are intended to be processed,
- (e) the law in force in the country or territory in question,
- (f) the international obligations of that country or territory,
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and (h) any security measures taken in respect of the data in that country or territory.

⁷⁷⁷ These include cases where the data subject has given consent to the transfer of such data and a fairly detailed list of other conditions similar to those in Schedules 2 and 3.

⁷⁷⁸ Cf the Preface to the Guidelines. See also Roos op cit at 156-157.

⁷⁷⁹ For instance, there is a clear link between the Second principle and the Third principle. Cf above Para 3.2.3 (iii). Cf Roos op cit at 170 where she points out that the principles embodied in the OECD Guidelines are all interrelated.

suggested that for practical purposes, as in the case of the OECD principles,⁷⁸⁰ and for enhanced coherence, the data protection principles enumerated in the DPA should be synchronised and applied as a whole rather than as separate disjunctive units.

3.2.3.2.2.5b Application to Internet Cafes

The principles enunciated above have been described as the basic principles of data protection.⁷⁸¹ In essence, they embody essential components to be included in any law for the protection of data and are generally and universally applicable for the protection of processed information. Regarding information processed in Internet cafes for instance, in line with the Second principle and the OECD Openness principle, it is important for customers in Internet cafes to know that personal information concerning them will be retained in computer memory and to have access to such information.

Also, in line with the Second principle and the OECD Purpose Specification and Use Limitation principles, it is essential for Internet café operators to specify the purposes for which information may be stored, retained, disclosed or otherwise used by them and to maintain processing within these limits. In line with the Third principle and the OECD Collection Limitation and Use Limitation principles, Internet café operators will also be required to ensure that data retained, collated, disclosed or otherwise processed by them is necessary and relevant to the purpose/s specified by them.

⁷⁸⁰ Cf above Para 3.2.3.2.1.2.

However, since Internet café operators do not directly collect information,⁷⁸² the Fourth DPA principle correlating to the OECD Collection Limitation and Use Limitation principles will not be directly relevant for the regulation of information processed in Internet cafes. Internet café operators will neither be obligated to verify the truth or accuracy of information processed on computers in their cafes, nor required to update records maintained on their computers. However, they will be required not to retain any information on their computers for longer than necessary, thus the Fifth principle (OECD Storage Limitation) principle will be relevant.

The Sixth principle which highlights the recognition of data subjects' rights is both relevant and crucial to the actual enjoyment of privacy/data protection with regard to information processed in Internet cafes. For effective protection, it is essential that Internet café owners acknowledge customers' privacy and data protection rights and that they (Internet café owners) be placed under a duty to comply with specific provisions guaranteeing such protection. In the absence of such duty, Internet café owners may minimum and

The Seventh principle, (the OECD Security Safeguards principle) is also relevant for the protection of information processed in Internet cafes. In a research conducted in Nigeria and South Africa⁷⁸³ the implementation of technical measures regarding Internet cafe

⁷⁸¹ Cf Roos op cit at 173, Bainbridge in Roos at 280. See also above Para 3.2.3.2.2.5.

⁷⁸² Although they are data controllers by reason of information accumulated and retained on computers in their custody, they are different from credit bureau and other government or private institutions whose functions expressly involve the collection of information and maintenance of records.)

⁷⁸³ Cf below Appendix.

computers was one of the suggestions given for the improvement of privacy protection in Internet cafes.⁷⁸⁴ This provision is particularly useful for information processed in Internet cafes where customers have only limited license for the use of the computers and are not ordinarily authorised to install any programs on them.

It is thus imperative that the primary responsibility for the provision of appropriate and adequate technical protective measures to guarantee the privacy of information processed by customers should be the Internet café operators'. However, it must be asserted that this duty will not relieve customers of their corresponding duty to ensure that they are properly logged out⁷⁸⁵ and to take such precautionary measures for their own privacy protection as may be available to them.

Lastly, the Eighth principle which prohibits international transfer of data will be relevant for the protection of information processed in Internet cafes. However, given the ease and freedom with which information is sent across countries via the Internet, the practical enforcement of this principle in Internet cafes will constitute a major challenge.⁷⁸⁶ It is submitted that even where Internet café operators comply with it, given the present Internet technology dispensation, there will continue to be gross violations of the Eighth

⁷⁸⁴ Cf below Appendix at Para 1.6.2a and 1.6.2b.

⁷⁸⁵ Cf Internet café owners and customers' responses in Paras 1.62a and 1.62b of the Appendix.

⁷⁸⁶ Cf the OECD requirement in Article 4 that on-line traders who process information via the computers of EU customers must follow European Union regulatory principles . (Above Para 3.2.3.2.1.3). It has been observed that there is not much development or jurisprudence on this aspect of the law. See Wikipedia Contributors Directive 95/46/EC on the protection of personal data http://en.wikipedia.org/wiki/directive_95/46/EC_on_the_protection_of_personal_data Accessed February 9, 2007.

principle by Internet users including customers in Internet cafes who communicate and transact business across nations.

3.2.3.2.3 Other Laws Protecting Data in the United Kingdom

There are a number of other laws containing provisions on data (and privacy) protection. A few of these Acts exemplifying certain areas relating to privacy and data protection will be briefly examined below.

3.2.3.2.3.1 The Consumer Credit Act⁷⁸⁷

The Consumer Credit Act⁷⁸⁸ governs consumer credit information. The Act provides protection in respect of information collected by credit reference agencies. It regulates information gathering and dissemination practices of credit reference agencies and allows individuals access to information processed by such agencies. For instance, the Act provides for disclosure by credit reference agencies of the name of their agencies,⁷⁸⁹ and places a duty on such agencies to disclose information contained in their files.⁷⁹⁰ The Act also provides for the correction of wrong information.⁷⁹¹

⁷⁸⁷ (1974) 11 Statutes 15.

⁷⁸⁸ (1974) 11 Statutes 15.

⁷⁸⁹ Section 157.

⁷⁹⁰ Section 158.

⁷⁹¹ Section 159.

The Data Protection Act 1998 has amended Sections 158 to 160 of the Consumer Credit Act 1974.⁷⁹² Section 158 deals with the duty of the agency to disclose filed information, section 159 provides for the correction of wrong information, and section 160 deals with alternative procedure for business consumers.

Section 62(1)(a) of the Data Protection Act amends Section 158 of the Consumer Credit Act, which requires an agency to disclose filed information, by providing for the substitution in Section 158(1) of the Consumer Credit Act of “individual” for “partnership or other unincorporated body of persons not consisting entirely of bodies corporate”, thus extending protection under that provision to groups of persons as well as individuals.

Section 62(2) of the Data Protection Act amends section 159 of the Consumer Credit Act, on the correction of wrong information. Section 62(2) (Data Protection Act) in essence provides for the erasure or destruction of incorrect information or information likely to prejudice the data subject. It provides for the substitution of subsection 1 of Section 159 (Consumer Credit Act), with “any individual, the ‘objector’.” It also widens the scope of the former provision by extending it to apply to information given under section 7 of the Data Protection Act by a credit reference agency,⁷⁹³ as well as information given under section 158 of the Consumer Credit Act.⁷⁹⁴

⁷⁹² Section 62.

⁷⁹³ Section 62(2) (a).

Section 62(3) of the Data Protection Act provides for the substitution of “consumer” in Section 158(2) to (6) with “the objector”⁷⁹⁵ and “director” with “the relevant authority”,⁷⁹⁶ thus expanding the scope of persons who may bring a complaint under the Act, as well as avenues for obtaining redress.

Section 62(5) of the Data Protection Act amends Section 160 of the Consumer Credit Act by providing for the substitution in subsection 4 of the Act, of “him” with “the consumer”, “his” with “the consumer’s”,⁷⁹⁷ and also provides that “consumer” has the same meaning as in section 158 of the Act.⁷⁹⁸ Generally, the effect of the Data Protection Act is to widen the scope of these provisions (Sections 158-160) of the Consumer Credit Act, to allow a wider category of people to bring complaints under the Act.

3.2.3.2.3.2 The Access to Medical Reports Act⁷⁹⁹

This Act provides guidelines for the disclosure of medical⁸⁰⁰ records. The Access to Medical Reports Act mainly makes provision for patients and other persons authorised by

⁷⁹⁴ Section 62(2)(b).

⁷⁹⁵ Section 62(3)(a).

⁷⁹⁶ Section 62(3)(b).

⁷⁹⁷ Section 62(5)(a).

⁷⁹⁸ Section 62(5)(b).

⁷⁹⁹ Chapter 28 of 1988.

⁸⁰⁰ Section 4 Access to Medical Records Act.

law (e.g. parents, guardians) to gain access to their medical reports, and as such contain limited provisions for the general protection of data.

Under Section 7 of the Act, a medical practitioner is not obliged to give access to information where the disclosure of a medical report or part thereof is likely to reveal information about another person, or to reveal the identity of another person who has supplied information to the medical practitioner about the individual.⁸⁰¹ The Access to Medical Records Act extends the protection given to computerized records under the 1984 Data Protection Act to manual records.⁸⁰²

3.2.3.2.3.3 The Access to Health Records Act⁸⁰³

This Act provides guidelines for disclosure of health records.⁸⁰⁴ Like the Access to Medical Reports Act, the Access to Health Records Act makes provision for patients and other persons authorised by law to gain access to their health records. The Access to Health Records Act is implemented by regulations.⁸⁰⁵

⁸⁰¹ Section 7(2).

⁸⁰² Cf Sections 68 & 69 Data Protection Act 1998.

⁸⁰³ Chapter 23 of 1990.

⁸⁰⁴ See generally Access to Health Records (Control of Access Regulation) 1993, SI1993/746.

⁸⁰⁵ Ibid.

3.2.3.2.3.4 The Official Secrets Act⁸⁰⁶

The Official Secrets Act⁸⁰⁷ provides penalties for spying which is “prejudicial to the safety or interests of the State”.⁸⁰⁸ Under the Act, it is an offence to obtain or communicate information where such information is calculated or intended to be “directly or indirectly useful to an enemy.”⁸⁰⁹

3.2.3.2.3a Relevance to Internet Cafes

The financial and health sector are pertinent to every individual thus the protection of information relating to medical and health records as well as financial information will be relevant. Further, following the USA twin tower bombings of September 11th, 2001, issues relating to the protection of the state, espionage, official secrets, have become more commonplace. The disclosure of information relating to health, finances or of state secrets in an Internet café will have far-reaching effects and may cause irreparable damage. It will thus be useful to have detailed provisions (supporting available legislation) on these areas in any Data Protection Act relating to Internet cafes.

3.3 Conclusion on the Law Protecting Privacy and Data in the United Kingdom

⁸⁰⁶ Chapter 6 of 1989.

⁸⁰⁷ Chapter 6 of 1989.

⁸⁰⁸ See generally Section 1.

⁸⁰⁹ Section 1(c).

3.3.1 Privacy Protection

In summing up, it is clear that in the United Kingdom, most of the privacy cases that were brought in English law succeeded on the basis of the principle of breach of confidentiality.⁸¹⁰ The cases examined also reveal that English Common law made some provision for substantive and informational privacy rights.⁸¹¹ In this regard, many of the cases of breach of confidentiality in family matters protected substantive privacy rights⁸¹² while cases of breach of confidentiality in business situations often protected informational privacy rights.⁸¹³ It has also been shown that juristic persons can enjoy informational privacy rights.⁸¹⁴ In *Argyll v Argyll*,⁸¹⁵ the court protected substantive as well as informational privacy rights.

However, for an action based on breach of confidence to succeed, a relationship of confidentiality must exist or be implied by the courts, otherwise there would be no remedy for the plaintiff, even where there had been an invasion of their privacy.⁸¹⁶

⁸¹⁰ Ibid.

⁸¹¹ See above Para 3.2.1.1.2.

⁸¹² *Albert v Strange* supra, *Francome v Mirror Group Newspapers Ltd* supra.

⁸¹³ *Morison v Moat* supra, *Thomas Marshall (Exports) v Guinle* supra, *Rolls Royce Ltd v Jeffrey* supra.

⁸¹⁴ See above Para 3.2.1.1.2.

⁸¹⁵ Supra.

⁸¹⁶ See above Para 3.2.1.1 ff.

Apart from the cases brought on the basis of confidentiality, some of the Common Law torts provided some privacy protection. Tort law privacy protection was however inadequate since an aggrieved person had to fit his or her case within one of the nominate torts to be heard. For instance, for an action based on trespass to person to succeed, there must be contact with, or the threat of imminent harm to, the plaintiff.⁸¹⁷

Similarly, in the case of trespass to land and trespass to chattel, there must be contact with the plaintiff's land or property,⁸¹⁸ and an action for trespass to land will only avail a plaintiff who has an interest in the land.⁸¹⁹ However, in many cases, it is not necessary to have any direct contact with people, neither is there always a threat of physical harm involved in the act of spying on people, or otherwise invading their privacy, and incidences of invasion of privacy are not limited to places where one has an interest in property.⁸²⁰

In the same vein, for an action in nuisance to succeed, it may be necessary to prove that the interference complained of by the plaintiff was continuous,⁸²¹ and in the case of private nuisance, the plaintiff must have an interest in the land.⁸²² The tort of defamation is designed to protect the plaintiff's reputation, but even where the plaintiff's privacy has

⁸¹⁷ Ibid.

⁸¹⁸ See above Para 3.2.1.2.1.

⁸¹⁹ *Kaye v Robertson* supra.

⁸²⁰ *Kaye v Robertson* supra, *Bernstein [of Leigh (Baron)] v Skyways & General Ltd* supra.

⁸²¹ See above Para 3.2.1.2.2.

⁸²² Ibid.

been invaded and his personality or reputation injured, in certain cases, there will be no remedy for the plaintiff if the defendant relies on the defense of justification and proves that the facts disclosed are true.⁸²³

In effect, even where there was a clear case of invasion of privacy, to give judgment for the plaintiff, the courts had to find other grounds for protecting the right to privacy.⁸²⁴ This placed a notable restriction on the “privacy type” cases that could be successfully brought and the protection that could be obtained for invasions of privacy was thus limited. The aggrieved party was also bound to accept whatever protection could be gleaned from the tort under which the action was brought irrespective of its effectiveness and benefit (or the lack thereof) in the circumstances. The absence of a separate tort of privacy thus left a gap in English law. These *lacunae* have now been filled by the Human Rights Act, which recognises the individual’s right to privacy in terms of the European Convention on Human Rights.

In conclusion, it may be said that the law on privacy protection in the United Kingdom has developed from little or no Common Law recognition affording limited privacy protection, to statute law recognition and an unequivocal guarantee of the right to privacy, which, so far, has been broadly interpreted and upheld.

3.3.1a Relevance to Internet Cafes

⁸²³ See above Para 3.2.1.2.3ff.

⁸²⁴ See *Kaye v Robertson* supra. Cf above Para 3.2.1.2.1ff.

The following may be concluded with regard to the relevance of English law for the protection of privacy in Internet cafes. Since the privacy protection afforded by the Common Law is limited, it will be more beneficial to look to the Human Rights Act for our purpose. In this regard, one must look to Article 8 of the European Convention on Human Rights which has been interpreted to cover both personal and business correspondence⁸²⁵ without any restrictive clause or exemptions as to the nature of the correspondence. Since the transfer of messages via electronic mail is actualized by means of a telephone line,⁸²⁶ it may be argued that electronic mail correspondence is correlative to telephonic correspondence under Article 8.

Article 8 of the ECHR may thus serve as an example of a broad-based provision that will enable an Internet café user a general right to privacy in respect of his/her personal or business correspondence or mail. In this case, the cases decided by the European court will also be useful for guidance in construing the ambit of such provision. Details of provisions to be included in a data protection law for Nigeria will be discussed below.⁸²⁷

3.3.2 Data Protection

⁸²⁵ *Niemetz v Germany* supra.

⁸²⁶ Cf Nicol et al op cit at 88.

⁸²⁷ Chapters 8 and 9.

In sum, the 1998 Data Act contains several positive features for effective data protection. These include the applicability of the Act to both paper and computer –held records,⁸²⁸ (thus including both the old and the new record forms), extensive provisions regarding rights of data subjects,⁸²⁹ duties of data controllers,⁸³⁰ definition of key terminology,⁸³¹ and the provision for a Data Commissioner⁸³² among others. The Act also contains other specific provisions for the enforcement of its provisions,⁸³³ for prosecutions, as well as penalties⁸³⁴ for offenders under the Act. Most significantly, the eight principles of data protection⁸³⁵ provide a universally applicable and firm basis for the general protection of data.

One major shortcoming of the Act however, is the fact that many of the powers conferred on the Data Commissioner for the protection of data subjects are to be exercised at his/her discretionary. As such, where there has been an infringement of a person's rights under the Act, such a person cannot compel action by the Commissioner, unless such infringement relates to one of the non-discretionary matters provided for by the Act.⁸³⁶ This greatly detracts from the force of the protection conferred by the Act and is a major

⁸²⁸ Section 1(1).

⁸²⁹ Part II.

⁸³⁰ Part III.

⁸³¹ Part I Section 1.

⁸³² Section 6.

⁸³³ Part V (Sections 46 & 47).

⁸³⁴ Sections 60 & 61.

⁸³⁵ Part 1 Schedule 1, United Kingdom Data Protection Act 1998. Cf above Para 3.2.3.2.2.5.

restriction on the rights that may be asserted by a data subject under the Act. In conclusion, the 1998 data Protection Act contains many valuable features and provisions for the protection of privacy but leaves a notable *lacuna* in the area of the enforcement of the Act.

3.3.2a Relevance to Internet Cafes

Many of the features of the 1998 Data Act pointed out above will be valuable in the preparation of data protection laws and/or laws for the protection of privacy in Internet cafes for Nigeria. For instance, the provision for a Data Protection Commissioner⁸³⁷ whose duties are provided for clearly and in detail⁸³⁸ enhances effective compliance with, and enforcement of, the Act and it is suggested that a similar arrangement could be considered in Nigeria. Also the provision making the Act applicable to both paper-based and computer-held records⁸³⁹ will be very functional in Nigeria.

Therefore, with regard to the utility of the Act for the protection of privacy in Internet cafes in Nigeria, it may be concluded that the 1998 Data Protection Act will be valuable in establishing general data protection principles in Nigeria and instructive regarding features to be included in a Data Protection Act, applicable in Nigerian Internet cafes.

⁸³⁶ Cf above Para 3.2.3.2.2.3.

⁸³⁷ Section 6.

⁸³⁸ Sections 51.

Having thus examined the Common Law in the United Kingdom, it is intended to examine the law in the United States America.

⁸³⁹ Section 1(1), Data Protection Act, Chapter 29 of 1998.

CHAPTER FOUR

PROTECTION OF PRIVACY AND DATA IN THE UNITED STATES OF AMERICA

4.1 Constitutional Protection of Privacy and Data

As in the case of the United Kingdom, it is intended to examine the relevant laws in the United States of America with the aim of extracting principles for the protection of electronic mail in Internet cafes, or/and, establishing general guiding principles for a Data Protection Law for Nigeria. The different aspects of the applicable law will be examined, followed by an overall conclusion on the categories examined.

4.1.1 Constitutional Protection of Privacy

Although the right to privacy is based on the Constitution in the United States of America, the word “privacy” does not appear in the Constitution,⁸⁴⁰ and no general right of privacy or personality is expressly provided for in the Constitution. The Constitution however contains several provisions limiting state and federal government activities in such a way as to protect the right to privacy. In particular, the provisions of the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments have been construed, each in a

⁸⁴⁰ See G S McClellan *The Right to Privacy* (1976) at 14.

different way, to protect privacy rights. Thus, it has been held that the right to privacy is guaranteed implicitly in the United States Constitution.⁸⁴¹

In *Griswold v Connecticut*,⁸⁴² the narrow protection of privacy derived from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments to the Constitution were cited. It was the opinion of the justices in *Griswold's* case that together, the Amendments to the Constitution formed a penumbra guaranteeing privacy. In *Roe v Wade*,⁸⁴³ previous decisions of the court recognizing that a right of personal privacy, or a guarantee of certain areas or zones of privacy under the Constitution, were cited.

Substantive and informational privacy rights are protected in the United States by the 1st, 3rd, 4th, 9th and 14th Amendments. These Amendments will be dealt with in turn.

4.1.1.1 First Amendment

The First Amendment prohibits the making of laws abridging freedom of speech and the right of assembly. In *NAACP v Alabama*,⁸⁴⁴ an Alabama State law, which required that a private association, that had been formed constitutionally, must reveal the names of its officers and members, was held to violate the provisions of the First Amendment. Here,

⁸⁴¹ *Griswold v Connecticut* (1965) 381 US 479.

⁸⁴² *Supra*.

⁸⁴³ (1973) 410 US 113, 93 SCt 705.

⁸⁴⁴ (1958) 357 US 449.

the court recognised a right to “associational privacy”- the right not to disclose details of groups or associations with which one associates. In *Bartnicki v Vopper*,⁸⁴⁵ the Supreme Court, relying on the First Amendment, held that a re-broadcast, by a commercial radio station of an illegally intercepted telephone conversation was unconstitutional. In these cases, informational privacy rights were protected by the First Amendment.

In *McIntire v Ohio Elections Committee*⁸⁴⁶ the right to anonymity was recognised by the courts on the basis of the First Amendment. Similarly, in *Watchtower Bible & Tract Society of N.Y. v Village of Stratton*,⁸⁴⁷ the Supreme Court invalidated a law requiring registration with the government in order to engage in door-to door soliciting, as violating the First Amendment right to anonymity.

It is noteworthy that the provisions of the First Amendment may be used as a double-edged sword to protect both the right to privacy and the right to access information.⁸⁴⁸ In *Reno v American Civil Liberties Union*,⁸⁴⁹ the Supreme Court held that the provisions of the Communications Decency Act,⁸⁵⁰ which sought to curtail the publication of potentially harmful material to children on the Internet, were unconstitutional on First

⁸⁴⁵ (2001) 532 US 514, 121 SCt 1753.

⁸⁴⁶ (1995) 115 US 1511.

⁸⁴⁷ (2002) 122 SCt 2080.

⁸⁴⁸ In *Bartnicki v Vopper* supra, the court also found that the content matter of the broadcast was of public concern.

⁸⁴⁹ (1997) 117 SCt 2329.

⁸⁵⁰ Title V of the Telecommunications Act (1996) Public Law No 104-104, Sec 502, 110 Stat 56, 133-135.

Amendment grounds. The Supreme Court upheld the right of adults to receive and address certain forms of speech to one another, which may be potentially harmful for children.⁸⁵¹

Similarly, in *McNamara v Freedom Newspapers*⁸⁵² a newspaper picture of the plaintiff chasing a soccer ball with his shorts falling down and exposing his genitalia was published in conjunction with an article reporting a school soccer game. The plaintiff's action failed and the court held that the defendants had accurately depicted a newsworthy event, and as such, were protected by the First Amendment.⁸⁵³

4.1.1.1a Relevance to Internet Cafes

The First Amendment will be relevant for the protection of information processed in Internet cafes in two ways. Firstly, in line with the decision in *Reno v American Civil Liberties Union*,⁸⁵⁴ it will be applicable in upholding the right of adults to access and receive pornography and other information via Internet cafes.

On the other hand and in line with *McNamara v Freedom Newspapers*,⁸⁵⁵ the First Amendment may also serve as a broad defence in cases where information is published

⁸⁵¹ See also *Sable Communications of California Inc. v FCC* (1989) 492 US 115.

⁸⁵² (1991) Tex App Corpus Christi 802 SW2d 901.

⁸⁵³ See also *Kolengas v Hefel Broadcasting Corp.* (1991 2d Dist) 217 I11 App 3d 863, 161 I11 Dec 172, 578 NE 2d 299; *Logan v Sears, Roebuck & Co.* (1985) 466 So.2d 121 (Ala.)

⁸⁵⁴ (1997) 117 SCt 2329.

⁸⁵⁵ *Supra*.

through an Internet café, or where information obtained through an Internet café is published.

4.1.1.2 Third Amendment

The Third Amendment provides: “No soldier shall in time of peace be quartered in any house without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.” By virtue of this provision, a person may not be compelled to provide asylum for soldiers in time of peace. This provision guarantees the privacy of a homeowner against intrusions that may be occasioned by the army.

The Third Amendment further states that where, by reason of war, it is necessary to quarter a soldier, this should be done within the law. This means that the constitutional, statutory and Common Law principles protecting privacy in the United States as well as any other relevant laws should be taken into consideration in cases where the need arises to quarter a soldier. Thus any act that would constitute an invasion of privacy under any relevant laws will also be illegal in such instances. Third Amendment rights generally protect substantive privacy interests.⁸⁵⁶

⁸⁵⁶ Cf D McQuoid-Mason “Privacy” in M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz, S Woolman (eds) *Constitutional Law of South Africa* (2004) at 38-23:

“Personal autonomy privacy enables individuals to decide who should enter their homes and protects individuals from unauthorised intrusions into their homes by officers of the state and other uninvited persons.”

Cf also the South African case of *State v Madiba* 1998 (1) BCLR 38, 43 (D).

4.1.1.2a Relevance to Internet Cafes

Although the 3rd Amendment bears no relevance to the protection of privacy or data in Internet cafes, the principle requiring the quartering of soldiers to be done within the law may be adopted for the regulation of information processed in Internet cafes. In effect, the processing of information in Internet cafes should be done in line with the provisions of the Nigerian Constitution on the right to privacy, relevant statutory provisions and applicable Common Law principles. Thus, any act that would constitute an invasion of privacy under Section 34 of the Nigerian Constitution,⁸⁵⁷ or violate a statutory provision protecting privacy,⁸⁵⁸ or, amount to a breach of any relevant Common Law principle⁸⁵⁹ will also be illegal when done in an Internet café.

4.1.1.3 Fourth Amendment

The Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.... ”.⁸⁶⁰ The United States Supreme Court has defined a search as a “governmental invasion of privacy.”⁸⁶¹ The law regarding what may constitute

⁸⁵⁷ Cf below Para 7.2.1.1.

⁸⁵⁸ Cf below Para 7.2.2.1.

⁸⁵⁹ Cf below Para 6.2.

⁸⁶⁰ Bill of Rights 1791; Cf H Henderson *Privacy in the Information Age* (1999) at 15.

⁸⁶¹ *Rakas v Illinois* (1978) 439 US 128 at 143, 99 SCt 421.

“unreasonable search” has however evolved with the advancement and proliferation of technological devices. In *Olmstead v U.S.*,⁸⁶² the U.S. Supreme Court held that telephone tapping did not constitute an unreasonable search within the ambit of the Fourth Amendment. However, in *Katz v United States*⁸⁶³ electronic eavesdropping on private conversations was held to constitute a search and seizure impinging on the privacy of conversation and therefore subject to Fourth Amendment requirements.

The position with regard to telephone tapping in the United States is that where interception of communication is to be done by the police, they must obtain a warrant, and private persons must obtain consent from the parties, or one of the parties to the conversation.⁸⁶⁴ In effect evidence obtained through a telephone tap will be admissible where the tap is conducted by the police under a search warrant, or by private persons with the consent of the parties or one of them.⁸⁶⁵ The only form of eavesdropping specifically forbidden is that done by third parties without the consent of any of the parties to the conversation.⁸⁶⁶

⁸⁶² (1928) 277 US 438.

⁸⁶³ (1967) 389 US 347. This decision reversed the Supreme Court’s decision in *Olmstead v U.S.* where the police placed a wiretap outside the plaintiff’s house, and this was held not to constitute a search within the scope of the Fourth Amendment. In *Katz*, the Supreme Court established that a person has a “reasonable expectation of privacy” in making a telephone call from their home and that the police must get a warrant in order to lawfully tap their telephone line.

⁸⁶⁴ *People v Shinkle* (1989) 128 III 2d 480, 132 III Dec 432, 539 NE2d 1238, where the testimony of a police officer was admissible, where he had heard the statements of the defendant on an extension phone with the consent of the other party to the conversation.

⁸⁶⁵ Cf the position in the United Kingdom. See Lord Goff in *Attorney General v Guardian Newspapers (No2)* [1990] 1 AC 109 at 281. See also Raymond Wacks *Privacy and Press Freedom* (1995) at 131.

In *Smith v Maryland*,⁸⁶⁷ the court ruled that the electronic monitoring of numbers dialed from a private telephone at the request of law enforcement officials without a search warrant did not constitute a Fourth Amendment search. The court was of the opinion that the dialer could have no reasonable expectation of privacy in respect of information because numbers dialed were transmitted to a third-party (the telephone company).

Similarly, in *United States v David Lee Smith*,⁸⁶⁸ the court ruled that conversations on cordless telephones without a search warrant were not protected by the Electronic Communications Privacy Act,⁸⁶⁹ and, did not constitute a Fourth Amendment search. However, statute law has also evolved with the advancement of technology to offer better protection for the right to privacy in this regard.⁸⁷⁰

Subsequent to these decisions, it appears that the courts have interpreted Fourth Amendment cases involving the use of technological equipment to effect searches, less restrictively.⁸⁷¹ However, the current position of the law with regard to the interception

⁸⁶⁶ See Statutory Protection of Privacy in the United States below Para 4.3.

⁸⁶⁷ (1979) 442 US 735, 61 L Ed 2d 220, 99 SCt 2577.

⁸⁶⁸ (1992) 978 F.2d 171, US App.

⁸⁶⁹ 1986. Cf below Para 4.3.1.12.

⁸⁷⁰ See below Para 4.3.1.1.2.

⁸⁷¹ See *U.S. v Karo* (1984) 468 US 705, where an electronic beeper that was activated in the plaintiff's house, which the police used to infer movement in the house was held to violate Fourth Amendment rights. See also *Kyllo v U.S.* (2001) 121 SCt 2038, where the court held that the use of a thermal imaging device without a warrant violated the plaintiff's Fourth Amendment rights.

of calls has been adversely affected by the PATRIOT Act 2001.⁸⁷² Certain provisions of the Act permit acts that would be an infringement of Fourth Amendment rights.⁸⁷³ By reason of the fact that it diminishes from the protection otherwise available for privacy, it is submitted that the provisions of the PATRIOT Act may also constitute an infringement of the Fourteenth Amendment which forbids the making or enforcing of any law that abridges the privileges or immunities of citizens.⁸⁷⁴

Searches in offices, schools and business environment, as opposed to the home, have been treated differently under the Constitution. In *New Jersey v T.L.O.*,⁸⁷⁵ a student was smoking in the school lavatory in violation of school rules. When she denied that she had been smoking, the vice-principal searched the student's purse and found marijuana and other articles in the purse that suggested that the student was dealing in marijuana. The court held that the search was permissible and did not constitute a violation of the student's Fourth Amendment rights.

The court noted that, although students have an expectation of privacy, searches that are reasonably related to suspected violations of rules would not constitute violations of the Fourth Amendment, where the measures adopted are "reasonably related to the objectives

⁸⁷² Public Law 107-56; 115 Stat 272 (2001). See below Para 4.3.1.13.

⁸⁷³ Sections 202 and 203. Cf Para 4.3.1.13 below.

⁸⁷⁴ Cf below Para 4.1.1.6 for cases on the Fourteenth Amendment.

⁸⁷⁵ (1985) 469 US 325.

of the search and not excessively intrusive in the light of the student's age, sex and the nature of the infraction."⁸⁷⁶

Similarly in *O'Connor v Ortega*⁸⁷⁷ the director of a State Hospital in California, suspecting that a psychiatrist in the employment of the hospital was engaging in certain unlawful activities, searched the psychiatrist's office and seized certain documents, (which were later used against Dr Ortega in proceedings), while he was on administrative leave. The court held that while employees had an expectation of privacy in the workplace, an employer did not need to obtain a warrant to search their employees' belongings at work, but only needed to meet a standard of reasonableness in order to conduct a search.

Generally in the United States, it appears that the right of employees to privacy in the workplace is limited.⁸⁷⁸ In line with this, mail sent or received at work is regarded as part of office work or documents, and employers are allowed to read their employees' mail.⁸⁷⁹ In *Alana Shoars v Epson America Inc.*,⁸⁸⁰ where a supervisor had been retrieving and printing out all the electronic mail sent by employees in one of the company's offices, the court established that employers have the right to monitor workplace e-mail.

⁸⁷⁶ At 340-341.

⁸⁷⁷ (1987) 480 US.

⁸⁷⁸ Cf Henderson op cit at 73.

⁸⁷⁹ *Alana Shoars v Epson America, Inc.*, (1990) No. 073234, La Sc.

⁸⁸⁰ Supra. Cf *Soroka v Dayton Hudson Corp.* (1991) 1 Cal Rep 2d 77, 6 IER Cases (BNA) 1491 App.

Although the sending and receiving of e-mail has become routine in offices, it is also trite that in offices, e-mail, like the telephone is often used for both official and private communications. It is arguable that an employee should have a measure of privacy in respect of private e-mails and as such, where the subject of any mail clearly indicates that such mail is of a personal nature, an employee should have a reasonable expectation of privacy with respect to such.

In line with this, it is suggested that a parallel can be drawn between e-mail and ordinary mail. Where personally addressed letters are received at work, or where a letter is marked “private and confidential”, such letters are generally regarded as personal and are left to be opened by the addressee. It is submitted that the same reasonable expectation of privacy should be accorded to e-mail where the subject line of such mail contains indications as to its private nature.

In *Katz v US*,⁸⁸¹ the Supreme Court, in giving judgment for the plaintiff, referred to a previous Supreme Court decision⁸⁸² establishing in effect that the Fourth Amendment protects people and not places, and that its provisions may be construed to constitutionally preserve and protect whatever a person (lawfully) seeks to preserve as private, even in an area accessible to the public such as a telephone booth or a business office.⁸⁸³

⁸⁸¹ *Supra*.

⁸⁸² *Silverman v US* (1961) 365 US 501. Cf C Anderson et al 115 *Harvard Law Review* (2001) No 1 at 352.

Following the same principle, it is submitted that the fact that a person receives e-mail in the office or through the use of office computers should not deprive such person of protection for his or her privacy, just as, receipt of non-electronic, or paper-based mail via an office address should not deprive mail so received of privacy protection.⁸⁸⁴

In *United States v Miller*,⁸⁸⁵ the court concluded that an individual has no Fourth Amendment expectation of privacy in respect of the information contained in cheques and deposit slips voluntarily entrusted to the bank because they flow between banks as part of ordinary commerce. The decisions in *United States v Miller* and *Smith v Maryland* have been criticised as wrong in principle, on the basis that they assume that the subscribers and clients have forfeited their right to privacy by agreeing to comply with statutory or other requirements of the service providers even if such requirements are unconstitutional.⁸⁸⁶

As can be seen from the cases, generally, Fourth Amendment rights protect informational privacy. However, the Fourth Amendment regulates searches in general, and this includes

⁸⁸³ *Silverman v US* supra at 511.

⁸⁸⁴ Cf the South African case of *Protea Technology Ltd & Anor v Wainer & Ors* 1997 (3) SA 694, where it was held that in matters not related to their employers' business, employees have a reasonable expectation of privacy with regard to telephone calls made and received by them. See also McQuoid-Mason in Chaskalson et al op cit at 38-34, where he affirms that unreasonable monitoring of employees' communications should be regarded as *prima facie* evidence of a breach of their constitutional right to privacy.

⁸⁸⁵ (1976) 425 US 435.

⁸⁸⁶ See McQuoid-Mason in Chaskalson et al op cit at 18-13 ; See also L du Plessis & J de Ville "Personal Rights" in D Van Wyk, J Dugard, B de Villiers, & D Davis (eds) *Rights and Constitutionalism: The New South African Legal Order* (1994) at 245.

the bugging of homes, which constitutes an unauthorised intrusion,⁸⁸⁷ as well as being a threat to individual autonomy. It is submitted that to the extent that the Fourth Amendment protects a person from unauthorized intrusions, protects personal autonomy and purports to allow people to act and make decisions with minimum interference, the Fourth Amendment also protects substantive privacy rights.

4.1.1.3a Relevance to Internet Cafes

The Fourth Amendment will be useful generally to protect against unlawful access by individuals or the government to information processed in Internet cafes. Thus it will be unlawful for any person to access the contents of a computer in an Internet café without legal justification. It will also be unlawful for Internet café personnel to read e-mail or other correspondence of customers without their consent.

The construction of the Fourth Amendment in *Silverman v US*⁸⁸⁸ is particularly useful in establishing grounds for the protection of information processed in Internet cafes because it addresses the issue of privacy invasion in public places. The principle laid down in *Silverman* extending privacy protection to whatever a person lawfully seeks to keep confidential even in publicly- accessible areas, is basic and valuable and it is suggested that this principle be included as a general test to determine whether or not to recognise a right to privacy in novel or complex Internet café related privacy cases in Nigeria.

⁸⁸⁷ Cf *McQuoid-Mason in Chaskalson et al op cit* at 38-22ff.

⁸⁸⁸ *Supra*.

4.1.1.4 Fifth Amendment

The Fifth Amendment provides that a person shall not be compelled to be a witness against himself in any criminal case. In effect, the government is prevented from compelling any individual to testify or give information for use in his or her criminal prosecution.⁸⁸⁹ This privilege against self-incrimination protects informational privacy. It protects against governmental intrusion into privacy with regard to information contained in one's mind.

The Fourth and Fifth Amendments have been described as providing protection against all governmental invasions of "the sanctity of a man's home and the privacies of life."⁸⁹⁰ It must be noted however, that the protection afforded by the Fifth Amendment is merely in respect of incriminating information. It does not afford general protection against the disclosure of private information.

4.1.1.4a Relevance to Internet Cafes

The Fifth Amendment will not be directly relevant for the protection of privacy or data in Internet cafes.

⁸⁸⁹ The *locus classicus* for this section of the Constitution is *Miranda v Arizona* (1966) 384 U.S. 436. See also *Re L.A.* (Kan 2001) 21P.3d 952, 961. Cf South African law, section 203 of the Criminal Procedure Act 51 of 1977 as amended, which also provides for privilege against self-incrimination. See below chapter 5.

4.1.1.5 Ninth Amendment

The Ninth Amendment provides: “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.” In *Griswold v Connecticut*,⁸⁹¹ the Supreme Court, relying on this provision, rejected the argument that the lack of a specific right of privacy in the Bill of Rights meant that no such right existed, and established that to determine whether a particular privacy right ought to be recognised, the United States courts ask themselves the question whether such a right is “implicit in the concept of ordered liberty”⁸⁹² in such a way that neither liberty nor justice would exist if it was sacrificed.

In deciding whether or not to recognise a given right, the courts also ask whether it is deeply rooted in the nation’s history and tradition.⁸⁹³ It has however been observed that this limitation narrows the scope of the right to privacy in the United States, compared to other jurisdictions.⁸⁹⁴ However, with regard to substantive and informational privacy

⁸⁹⁰ *Boyd v U.S.* (1896) 116 US 616.

⁸⁹¹ *Supra*.

⁸⁹² *Griswold v Connecticut* *supra* at 524; *Bowers v Hardwick* 478 (1986) US 186, 92 L Ed 2d 140, 146, 106 SCt 2481.

⁸⁹³ *Bowers v Hardwick* *supra*.

⁸⁹⁴ See *Bowers v Hardwick* *supra*. See also du Plessis & de Ville Van Wyk et al op cit at 243. Cf the South African case of *National Coalition for Gay and Lesbian Equality & Others v Minister of Justice & Others* (1998) 6 SACR 102 (W), where a law that made it an offence for a male to do an act calculated to stimulate sexual passion or give sexual gratification to another male at a party was declared invalid. The basis of the decision was however not the right to privacy but provisions guaranteeing equality in section 8 of the South African Interim Constitution.

rights, the provision of the Ninth Amendment may be used for the protection of both categories.

4.1.1.5a Relevance to Internet Cafes

The application of this principle for the protection of information processed in Internet cafes in Nigeria will require the courts to acknowledge and recognise other rights or benefits conferred by other relevant constitutional provisions or other laws. Section 36 of the Nigerian Constitution⁸⁹⁵ specifically provides for the right to privacy. Application of the Ninth Amendment would require positive acknowledgement and affirmation of other constitutional provisions that are relevant in the consideration of Section 36 privacy rights.

In essence, in giving effect to the constitutional right to privacy, other relevant constitutional rights such as the right to freedom of expression,⁸⁹⁶ the right to dignity,⁸⁹⁷ right to liberty⁸⁹⁸ and others must be recognised and upheld. Thus, in determining liability where, for instance, information is unlawfully published or disclosed in or through an Internet cafe, the right to privacy must be weighed against the right to freedom of expression if applicable in the case.

⁸⁹⁵ 1979 Constitution FRN.

⁸⁹⁶ Section 38.

⁸⁹⁷ Section 33.

⁸⁹⁸ Section 34.

4.1.1.6 Fourteenth Amendment

The Fourteenth Amendment forbids the making or enforcing of any law that abridges the privileges or immunities of citizens. In *Griswold v Connecticut*,⁸⁹⁹ the Supreme Court, relying on this provision, held that a law prohibiting the use of contraceptive devices interfered with the privacy of the marital relationship.

In *Roe v Wade*,⁹⁰⁰ a majority of the Supreme Court adopted the view that the right to privacy is “founded on the Fourteenth Amendment’s concept of personal liberty”.⁹⁰¹ In this case, the court decided that a law that prohibited abortion, except for the purpose of saving the mother’s life⁹⁰² was unconstitutional and that a woman had the right to privacy in respect of the decision whether or not to have an abortion. In both cases above, the Fourteenth Amendment was used to uphold substantive privacy rights. The provision of the Fourteenth Amendment is however broad, and may be used to protect informational privacy rights where appropriate.

It must be noted with regard to the constitutional protection of privacy, that there are also State Constitutions, which contain provisions recognising a right to privacy. For instance,

⁸⁹⁹ *Supra*.

⁹⁰⁰ (1973) 410 US 113, 93 SCt 705.

⁹⁰¹ At 129.

⁹⁰² This decision was refined in *Planned Parenthood of Southeastern Pennsylvania v Casey*, (1992) 112 SCt 931, 112 SCt 2791, where the Supreme Court found that a state statute that placed an undue burden on a woman’s decision to procure an abortion was unconstitutional. The Court held that the strict scrutiny test (see above 3.3.1.1 (a)) should not apply in cases of restrictions on abortions.

in Alaska the Constitution provides that “the right of the people to privacy is recognised and shall not be infringed”.⁹⁰³ In Arizona, the Constitution provides: “No person shall be disturbed in his private affairs or his home invaded, without authority of law”⁹⁰⁴ In New York, the first paragraph of the privacy provision, that states *inter alia*: “[T]he right of the people to be secure in their persons, houses, papers and effects, and against unreasonable searches and seizures, shall not be violated” is identical to the Fourth Amendment of the U.S. Constitution.⁹⁰⁵

4.1.1.6a Relevance to Internet Cafes

The provisions of the Fourteenth Amendment may be used as a shield to buffer the constitutionally guaranteed right to privacy in Nigeria. For our purpose, application of the Fourteenth Amendment would signify that laws prohibiting privacy protection with regard to information processed in Internet cafés are prohibited from being made, and where they already exist, they should not be enforced. In effect, any law which constitutes an infringement on, or, disregards, nullifies or purports to nullify privacy protection with regard to information processed in Internet cafes in Nigeria will be invalid and unenforceable.

⁹⁰³ Art.I sec. 22, Alaska Constitution (1972).

⁹⁰⁴ Art. II., sec. 8, Ariz. Constitution, 1912. See also Art. I, sec 1, Cal. Constitution.; DEL. Code tit.ii, sec. 1335; Art. I, sec. 12, Fla. Constitution ; Ga. Code Ann. Sec. 3001.

⁹⁰⁵ See Art. I, sec. 12, N.Y. Constitution.

4.1.2 Constitutional Protection of Data in the United States

As with the right to privacy, there is no general provision for the protection of data in the Constitution, but certain provisions have been construed to protect data, for instance the First and Fourteenth Amendments. Constitutional protection of data generally relates to informational privacy rights.

First Amendment rights have been interpreted by the Supreme Court to cover the collection of data. In *NAACP v Alabama*⁹⁰⁶ the court, relying on First Amendment rights, up-held the non-disclosure of the names and addresses of the members of an association. In *Whalen v Roe*,⁹⁰⁷ on the basis of the Fourteenth Amendment, the Supreme Court recognized a right of non- disclosure of personal matters.⁹⁰⁸ However, in balancing the individual's interest against the State's,⁹⁰⁹ the court, in this case, held that the State's interest in gathering information outweighed the individual's privacy interest.⁹¹⁰

4.1.2a Relevance to Internet Cafes

⁹⁰⁶ Supra.

⁹⁰⁷ (1977) 429 US 589.

⁹⁰⁸ At 598-600.

⁹⁰⁹ Cf above Para 1.1.

⁹¹⁰ Cf *Nixon v Administrator of General Services* (1977) supra.

Considering that, as in the United States, there is no constitutional provision guaranteeing the protection of data in Nigeria,⁹¹¹ it is suggested that the constitutional provisions regarding privacy protection in Nigeria⁹¹² be construed by the courts for the protection of data where practicable. Thus, for our purpose, the provisions of Section 36 of the Nigerian Constitution will also be construed for the protection of information or data processed in Internet cafes where applicable.

4.2 Common Law Protection of Privacy and Data in the United States

4.2.1 Common Law Protection of Privacy

The right to privacy was recognised at an early stage in some parts of the United States.⁹¹³ The inclusion of the right in the *Restatement of Torts*⁹¹⁴ brought wider recognition and acceptance by other jurisdictions.⁹¹⁵ Today, almost all 50 states recognise a civil right of action for invasion of privacy in their laws.⁹¹⁶ The rights recognised and

⁹¹¹ Cf below Para 7.2.1.2.

⁹¹² Section 36, 1979 Constitution FRN.

⁹¹³ The publication by Samuel Warren and Louis Brandeis of their famous article in which they described the right to privacy as “the right to be let alone” (at 195) brought legal recognition of a right to privacy to the limelight. See Warren & Brandeis “The Right to privacy” (1890) 4 *Harvard Law Review* 193. Cf D J McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 35.

⁹¹⁴ Section 867 *Restatement of Torts* (1939)

⁹¹⁵ McQuoid-Mason op cit at 37.

⁹¹⁶ R.E. Smith *Compilation of State and Federal Privacy Laws* (1997) <http://www.epic.org/privacy/consumerstateshtml> See also Keeton op cit at 851.

protected have been categorised into the following four groups by Prosser: intrusions, publication of private facts, putting a person in a false light and appropriation.⁹¹⁷

(1) INTRUSIONS

Intrusions have been defined as “intentional interference with another’s interest in solitude or seclusion either as to his person or to his private affairs or concerns.”⁹¹⁸ It includes intrusions upon physical solitude or illegal searches and extends to eavesdropping.⁹¹⁹

In *Dietemann v Time Inc*⁹²⁰ the defendants posed as prospective patients to gain access to the plaintiff’s office and subsequently used a hidden camera and microphone to record the plaintiff’s fake medical practice. The court held that the use of the recording devices was an actionable intrusion. However, the plaintiff in this case could not recover damages for the defendants’ physical intrusion. The court held that the plaintiff had no cause of action for the plaintiff’s physical intrusion as he had held his home open to patients. In

⁹¹⁷ W L Prosser “Privacy” (1960) 48 *Cal LR* 389; See also W P Keeton, D B Dobbs, R E Keeton & D G Owen *Prosser and Keeton on the Law of Torts* (1984) at 851ff.

⁹¹⁸ See Comment a, American Law Institute *Second Restatement of Torts* (1977) Section 652B which provides as follows:

“Intrusion upon seclusion. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person”

⁹¹⁹ Comment a, American Law Institute *Second Restatement of Torts* (1977) Section 652B.

⁹²⁰ 449 F.2d 245 (9th Cir, 1971).

other words, he was deemed to have given consent to the presence of the defendants on his property as potential patients. Thus, it appears that where access to the disclosed information is provided willingly by the plaintiff, he or she will be deemed to have given consent to the intrusion.

Similarly, in *Miller v Motorola*⁹²¹ where sensitive medical information about the plaintiff was disclosed by her employer to co-workers, this was held not to be an intrusion as the plaintiff had voluntarily provided the information to the employer. It is submitted that, an employee's voluntary provision of information to an employer should not justify, or exclude the employer from liability for, wrongful use of such information. It is further submitted that the principle established in criticizing the decision in *U.S. V Miller*⁹²² is applicable here: Employees should not be regarded as having forfeited their privacy rights by reason of having supplied information in compliance with work requirements.

For the tort of intrusion, to be successfully invoked, the act complained of must be of a highly offensive nature to a reasonable person.⁹²³ It is has however been pointed out that it is possible to interfere with a plaintiff's interest in solitude and to cause embarrassment, ridicule, shame, or otherwise occasion injury or damage to the plaintiff, without achieving the required threshold of offensiveness.⁹²⁴ For instance, in *Cape Pubs. Inc. v*

⁹²¹ 560 NE 2d 900 (1990 III App Ct).

⁹²² *Supra*. Cf above Para 4.1.1.3.

⁹²³ *Second Restatement of Torts* (1977) Section 652B.

⁹²⁴ See D A Anderson "The Failure of American Privacy Law" in B Markesinis (ed) *Protecting Privacy* (1999) at 150.

Bridges,⁹²⁵ the plaintiff's picture was taken when she was fleeing from a terrorist nearly naked and the picture was subsequently published on the front page of her home-town newspaper. The court was of the opinion that the photo showed no more flesh than was displayed by some women on the beach (irrespective of the fact that the plaintiff found the publication intrusive and had suffered embarrassment).

In this regard, the use of the concept of the "ordinary reasonable person" as well as "community mores" to determine whether or not there will be liability in respect of the act complained of has been criticised on the grounds that it is self-defeating and that it does not take into account context and individual sensibilities.⁹²⁶

(2) PUBLICATION OF PRIVATE FACTS

Publication of private facts occurs where private information is given publicity of a highly objectionable kind, or is not of legitimate concern to the public even if the information is true.⁹²⁷ Thus in *Melvin v Reid*⁹²⁸ where a film drew upon the plaintiff's

⁹²⁵ 423 So 2d 426 (1982 Fla App). See also *McNamara v Freedom Newspapers* supra which involved the publication of a photograph showing the plaintiff with his genitalia exposed while chasing a soccer ball during a football match.

⁹²⁶ Anderson in Markesinis op cit at 150. See *Cape Pubs. Inc. v Bridges* supra.

⁹²⁷ See Section 652D Restatement (Second) of Torts, which provides:

"Publicity given to private life. One who gives publicity to a matter concerning the private life of another is subject to liability to the other for the invasion of his privacy, if the matter publicised is of a kind that:

- (a) would be highly offensive to a reasonable person, and
- (b) is not of legitimate concern to the public"

⁹²⁸ (1931) 112 Cal App 285, 297. Cf also Keeton et al op cit at 856.

past life as a prostitute, the court upheld her right to privacy as a person who had reformed and given up her previous career.

Although the tort of public disclosure of private facts under which a person can obtain a remedy for unwanted disclosures is recognised in almost every state in the United States, it appears that the plaintiff in many a case does not get protection or redress, as the defences available to the defendant are often successfully raised. In this regard, Roos observes⁹²⁹ that the requirement of publication to the public at large brings the tort into conflict with the Constitutional guarantee of freedom of speech contained in the First and Fourteenth Amendments of the United States Constitution.

Thus in *The Florida Star v B.J.F.*⁹³⁰ where the plaintiff, a rape victim had been clearly named in a newspaper article, the court held that the article involved a matter of public significance and the defendant's defence of public concern succeeded.

(3) FALSE LIGHT

Publicity that places a person in a false light in the public eye has been described as publicity that is objectionable to the ordinary reasonable man and does not amount to

⁹²⁹ Op cit at 36.

⁹³⁰ (1989) 491 US 524, 536-7. See also *Ross v Midwest Communications Inc.* (1989) CA 5 Tex 870 F2d 271, 16, *Media LR* 1463. Cf *McNamara v Freedom Newspapers* supra.

minor inaccuracies.⁹³¹ However, it has been observed with regard to the publication of personal information, that the information published will often be true.⁹³² The requirement that the information published must be false is thus a disadvantage to plaintiffs in many cases and it has been observed⁹³³ the tort of false light is of limited practical use.

(4) APPROPRIATION

Appropriation of the plaintiff's name or likeness for the defendant's benefit or advantage is the fourth interest protected by the law of privacy.⁹³⁴ It has been held that to use a person's distinctive nickname,⁹³⁵ slogan⁹³⁶ or costume⁹³⁷ will amount to appropriation.⁹³⁸

⁹³¹ See Para 652D" See section 652E *Restatement* (Second) of Torts, which provides:

"Publicity placing person in false light. One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if:

- (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
- (b) the actor had knowledge or acted in reckless disregard as to the falsity of the publicised matter and the false light in which the other would be placed"

⁹³² Cf *Dempsey v National Enquirer* 702 F.Supp.934 (D.Me.1989). Cf Keeton et al op cit at 863.

⁹³³ Roos op cit at 35 - 36.

⁹³⁴ See Section 652C *Restatement* (Second) of Torts, which provides:

" Appropriation of name or likeness. One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy"

⁹³⁵ *Hirsch v S.C. Johnson & Sons Inc.* 90 Wis. 2d 379, 280 NW2d (1979).

⁹³⁶ *Carson v Here's Johnny Portable Toilets Inc.* 698 F2d 831 (6th Cir. 1983).

⁹³⁷ *Motschenbacher v R.J Reynolds Tobacco Co.* 498 F2d 821 (9th Cir. 1974).

As in the case of the false light tort, the tort of appropriation also affords only limited privacy protection because its primary aim is the protection of proprietary interest.⁹³⁹

It has been observed⁹⁴⁰ generally that under American tort law, the majority of cases where the plaintiff has received protection for invasion of privacy, and where the courts have actively interpreted or expanded the scope of the right to privacy, have been in respect of the plaintiff's right to recover damages for commercial exploitation.⁹⁴¹ In line with this, the right to commercial exploitation has been held to outlast a person's life,⁹⁴² whereas the courts have generally held that other privacy rights are terminated at the person's death.⁹⁴³ This has been criticized as suggesting that the courts are more eager to protect economic interests than those that cannot be monetarily quantified.⁹⁴⁴

Traditional Common Law doctrines also provide limited protection for the right to privacy. Under the law of trespass, people have the right to exclude others from their

⁹³⁸ See generally *Pavesich v New England Life Insurance Co* 122 Ga.190, 50 SE 68 (1905). Cf Keeton et al op cit at 851.

⁹³⁹ Roos op cit at 35 - 36.

⁹⁴⁰ See generally Anderson in Markesinis op cit at 138ff.

⁹⁴¹ Anderson in Markesinis op cit at 138ff. Cf *Factors Etc. Inc. v Pro Arts Inc.* 579 F2d 215 (2nd Cir. 1978); *Onassis v Christian Dior- New York Inc.* (1984) 472 NYS 2d 254; *Midler v Young & Rubicam* supra. Cf *Cape Pubs. Inc. v Bridges* supra.

⁹⁴² *Factors Etc. Inc. v Pro Arts Inc.* supra, where the court held that the corporation to which a pop star had assigned his rights had the right to exploit the commercial value of his personality after his death.

⁹⁴³ See *Restatement (Second) of Torts* Article 6521. Cf the *Mephisto* case BGH 20.3 (1968), 30 BverfGE 173 (1971), where the German courts granted posthumous protection to personality. See generally Anderson in Markesinis op cit at 140ff.

⁹⁴⁴ See Anderson in Markesinis op cit at 138.

property. The protection afforded by the law of trespass is however limited and may not cover cases of electronic intrusion and other cases for instance, where there is insufficient contact to uphold a claim for trespass,⁹⁴⁵ or where the plaintiff may be deemed to have given consent to the presence of the defendant on his or her property.⁹⁴⁶

The tort of intentional infliction of emotional distress may also provide some protection for the right to privacy in rare cases, where a person's privacy is invaded by outrageous means or for the sole purpose of harming the person. Thus where a radio station promoted a "dog of the week" show based on bridal photos in the newspaper and labelled the plaintiff too ugly to rate, the plaintiff was awarded damages for intentional infliction of emotional distress.⁹⁴⁷

This tort is however often unsuccessfully invoked in many cases as the courts have often held that the behaviour in question is not outrageous enough to cause emotional distress.⁹⁴⁸

4.2.1a Relevance to Internet Cafes

⁹⁴⁵ Cf the English case of *Bernstein [of Leigh (Baron)] v Skyways & General Ltd* supra.

⁹⁴⁶ Cf *Dietemann v Time Inc* supra.

⁹⁴⁷ *Murray v Schlosser* (1990) 574 A.2d 1339

⁹⁴⁸ In *Cape Pubs. Inc. v Bridges* 423 So.2d 426 (1982 Fla. App.), Cf *McNamara v Freedom Newspapers* supra.

Under the United States Common Law principles, there will be limited protection for privacy in Internet cafes generally where there is an intrusion in invading the plaintiff's privacy; where private information is given publicity of a highly objectionable kind; where publicity (or publication of information) places a person in a false light; and, where the use of information about the plaintiff amounts to appropriation. Thus where, for instance, information is unlawfully copied from computers in an Internet café, there will be liability in respect of such intrusion. Also, where personal information is obtained from Internet café sources and given publicity of a highly objectionable nature, there will be liability for such publication.

It may be said generally that the tort of intrusion will be useful to protect against wrongful access to information (including that contained in electronic mail), while publication of private facts, false light and appropriation will protect against wrongful use of information.

The traditional torts may also provide some protection with regard to information processed in Internet cafes. The protection afforded by traditional torts will however be limited in terms of the factors that must be proved in order to successfully bring an action based on the relevant tort (for instance, in the case of trespass where physical contact with the plaintiff's property must be present). Thus the tort of trespass will only afford protection where invasion of privacy involves contact with the plaintiff's property, for example where the defendant takes the plaintiff's floppy or flash disk containing personal information.

4.2.2 Common Law Protection of Data

There is little or no Common Law protection for data in the United States. Common Law data protection may be found only where the law of privacy also protects data. For instance, where data infringement amounts to publication of private facts⁹⁴⁹ or appropriation,⁹⁵⁰ or where there is an intrusion in obtaining the data in question,⁹⁵¹ or where the use of the data places the plaintiff in false light.

4.2.2a Relevance to Internet Cafes

The United States Common Law principles will be useful for the protection of data in Internet cafes where there is an intrusion upon Internet café premises in obtaining data, where data infringement perpetrated through the use of Internet café facilities amounts to appropriation or publication of private facts, or where the use of the data obtained or processed by means of Internet café facilities places the plaintiff in a false light.

4.3 Statutory Protection of Privacy and Data in the United States

⁹⁴⁹ Cf *Melvin v Reid* supra.

⁹⁵⁰ For instance, where the plaintiff is impersonated to obtain information about him/her. See *Goodyear Tire & Rubber Co v Vandergriff* (1936) 62 Ga App 662.

⁹⁵¹ For instance, where there is an unlawful entry on the land of the plaintiff in order to obtain and wrongfully use information about him/her, or where the plaintiff's correspondence is unlawfully read. Cf *Dietemann v Time Inc* supra. Cf the South African case of *S v Hammer & others* 1994 (2) SACR 496 (C) at 498.

In view of the fact that the main federal legislation available on privacy and data, (the Privacy Act⁹⁵² and the Freedom of Information Act⁹⁵³), are equally applicable for the protection of both data and privacy, the statutory protection of privacy and data will be treated together. A variety of other laws⁹⁵⁴ also protect specific areas of information such as financial records, credit reports, educational records, telephone records, cable television, video, children and the Internet, and motor vehicle registration. Federal laws will be examined separately from state laws.

4.3.1 Protection of Privacy and Data under Federal Laws

4.3.1.1 The Privacy Act of 1974⁹⁵⁵

The Privacy Act of 1974 regulates Federal Government information practices, which affect informational privacy. It protects records held by United States Government agencies.⁹⁵⁶ The Act provides that records maintained by agencies must be as accurate, relevant, timely and complete as is reasonably necessary to ensure fairness to the individual to whom the information relates.⁹⁵⁷ In *Bechhoefer v U.S. Dept of Justice Drug*

⁹⁵² (1974) 5 USC Section 552a, as amended.

⁹⁵³ (1966) 5 USC Section 552 as amended.

⁹⁵⁴ See below Paras 4.3.1.3 ff.

⁹⁵⁵ (1974) 5 USC Section 552a, as amended.

⁹⁵⁶ Section 551 (1), Section 552(f). In *Ditman v California* 191 F 3d 804 (9th Cir 1999), it was established that the Privacy Act is only applicable to federal agencies. See also *Perez-Santos v Malave* 23 Fed App 11 (1st Cir. 2001).

⁹⁵⁷ Section 552a(e)(5).

Enforcement Admin.,⁹⁵⁸ the court established that records include any information about the individual that is linked to that individual through an “identifying particular”.

In *Tobey v NLRB*,⁹⁵⁹ it was held that records must both be about a specified individual and must include a name or other “identifying particulars” relating to that individual. Thus in *McGregor v Greer*,⁹⁶⁰ where a letter containing the reasons for an employee’s discharge was retained in the Department of Education’s records, it was held that this did not violate the employee’s rights under the Privacy Act as the information was not retrievable by the employee’s name or other personal identifying particulars relating to the employee.

The Privacy Act also sets out principles to ensure that information is only used for the purpose for which it is obtained.⁹⁶¹ The Act requires agencies that collect data on individuals to inform the individuals that such data is being gathered;⁹⁶² to explain the purpose for the data collection;⁹⁶³ to tell them whether disclosure of information by them is mandatory or voluntary;⁹⁶⁴ and to provide them with other similar protective

⁹⁵⁸ 209 F3d 57 (2d Cir. 2000).

⁹⁵⁹ 40 F3d 469 (Dc Cir. 1994).

⁹⁶⁰ 748 F Supp 881(DC 1990).

⁹⁶¹ Section 552a (e), which generally provides for Agency requirements, particularly Section 552a(e)(6) & (7). See *National Federation of Fed. Employees v Greenberg* 789 F Supp 430 (DDC 1992).

⁹⁶² Section 552a(e)(3)(A).

⁹⁶³ Section 552a(e)(3)(B).

⁹⁶⁴ Section 552a(e)(3)(A).

warning.⁹⁶⁵ In addition, the Act establishes rules governing the use and disclosure of personal information⁹⁶⁶ and provides legal remedies that permit an individual to seek enforcement of the rights granted under it.⁹⁶⁷

With regard to available remedies under the Act, these usually take the form of court injunctions and/or an award of damages for the plaintiff.⁹⁶⁸ Damages will be awarded in respect of suits concerning the accuracy of information held on an individual,⁹⁶⁹ while the courts will grant injunctions in respect of actions to allow an individual to gain access to improperly withheld records,⁹⁷⁰ or, actions for the amendment of an individual's records.⁹⁷¹ It has been held that a court may order an equitable relief of expungement of records under the Act.⁹⁷² Although there may be a criminal prosecution for unlawful disclosure of records under the Act,⁹⁷³ it has been established that violations of the Act do not attract any relief during a federal criminal prosecution.⁹⁷⁴

⁹⁶⁵ See generally subsection (e) on agency requirements.

⁹⁶⁶ Section 552a(b), which regulates conditions of disclosure and Subsection (c) on accounting of certain disclosures.

⁹⁶⁷ Section 552a(g), which provides for civil remedies.

⁹⁶⁸ Section 552a(g)(1)(D).

⁹⁶⁹ Section 552a(g)(1)(C).

⁹⁷⁰ Section 552a(g)(1)(B). See *Edison v Dept of the Army* 672 F 2d 840 (11th Cir. 1982).

⁹⁷¹ Section 552a(g)(1)(A). See generally *Quinn v Stone* 978 F 2d 126 (3rd Cir. 1992).

⁹⁷² Action for expungement of records may also be brought under the Constitution. (*Doe v U.S. Air Force* 812 F2d 738, 741 (DC Cir. 1987)).

⁹⁷³ *U.S. v Gonzales* (No 76-132) (MD La Dec 21, 1976). See also *U.S. v Trabbert* 978 F Supp 1368 (D Colo 1997).

⁹⁷⁴ *United States v Bressler* 772 F 2d 287 (7th Cir. 1985).

The 1974 Privacy Act allows the public to know what information about them is available to the Government or other agencies, through the Government's information-collecting agencies.⁹⁷⁵ In *Sutton v Providence St Joseph Medical Center*,⁹⁷⁶ the courts established that private entities are not subject to the Act and cannot be held liable under its provisions. The Privacy Act also enables individuals to exercise better control over the information about themselves by authorizing the subject of information to obtain access to it,⁹⁷⁷ restricting the disclosure of information without the consent of the subject of the information,⁹⁷⁸ (except in certain specified circumstances),⁹⁷⁹ and by generally regulating the data collection practices of agencies.

The Act prescribes that an agency must collect information from the subject as far as is practicable when information may result in an unfavourable decision for the subject under a Federal programme.⁹⁸⁰ In effect, the Act enables individuals to take measures to protect their privacy in terms of the information or data kept by the government.

⁹⁷⁵ Section 552a(e)(4).

⁹⁷⁶ 192 F 3d 826 (9th Cir. 1999). See also *UNT v Aerospace Corp* 765 F2d 1440 (9th Cir. 1985).

⁹⁷⁷ Section 552a(d), which provides for access to records.

⁹⁷⁸ Section 552a(b). In *Pilon v US Dept of Justice* 73 F3d 1111, 1117-1124 (DC Cir. 1996), where the Justice Department transmitted records to a former employee of the agency, who had previously come into contact with the records as an employee of the agency in the course of duty, the court held that the transmission constituted a disclosure for which the Justice Department was liable under the Privacy Act.

⁹⁷⁹ Section 552a(b)(1)-(12)

⁹⁸⁰ Section 552(a)(e)(2). In *Waters v Thornburgh* 888 F 2d 870 (DC Circ. 1989) 874, where the supervisor of an employee of the Justice Department sought and received information from a state board of law examiners, in order to investigate suspicions concerning the employee's unauthorised use of administrative leave, the court found that there had been a violation of this provision of the Act.

However, it appears that the courts have tended to interpret certain provisions of the Act strictly, thereby restricting the scope of the protection that might be available for privacy. For instance, with regard to the requirement that records maintained by agencies must be such as is reasonably necessary to ensure fairness,⁹⁸¹ it has been held reasonable for an agency to maintain records, based on information conveyed by the state and local authorities, of sexual misconduct containing an unsubstantiated allegation without conducting its own investigation.⁹⁸²

Similarly, it has been held, with regard to the provisions on rectification and amendment,⁹⁸³ that, statements amounting to subjective evaluation are not subject to amendment.⁹⁸⁴ Notably, with regard to an individual's right to access information improperly held by an agency, and the right to amendment of information, it has been established that an agency cannot enjoin an agency to disclose information under the Act.⁹⁸⁵ In this regard, it has been held that the Act merely authorises a court to grant an injunction to enable an individual to gain access to, or, and to amend information. The Act does not imply that the court may grant broad injunctive relief.⁹⁸⁶

⁹⁸¹ Section 552a(e)(5); Section 552a(e)(1), and (e)(7).

⁹⁸² *Jones v U.S. Dept of Treasury* No 82-2420 (DDC Oct 18, 1983; 744 F 2d 878 (DC Cir. 1984). Cf *Graham v Hawk* 857 F Supp 38 (WD Tenn 1994); 59 F 3d 170 (6th Cir. 1995).

⁹⁸³ Section 552a.

⁹⁸⁴ *Reinbold v Evers* 187 F 3d 348 (4th Cir. 1999); *Webb v Magaw* 880 F Supp 20 (DDC 1995).

⁹⁸⁵ See *Wanbun Inini v Sessions* 900 F 2d 1234 (8th Cir. 1990), *Parks v IRS* 618 F 2d 677 (10th Cir. 1980).

⁹⁸⁶ *Ibid.*

The Privacy Act applies to citizens of the United States as well as foreigners who have been lawfully admitted for permanent residence.⁹⁸⁷ To this extent, it would appear that juristic persons are excluded from the purview of the Act.⁹⁸⁸ However in *Reticel Foam Co v U.S. Dept of Justice*,⁹⁸⁹ it was established that a corporation may bring an action prohibiting an agency from disclosing investigative information about it. The 1974 Privacy Act has been amended to keep up with technological developments. In 1988, the Act was amended to accommodate new laws regulating data “matching”⁹⁹⁰ and it was amended again in 1991.⁹⁹¹

It is noteworthy that, apart from the administrative officials who carry out specified administrative duties under the Act, the Act does not provide for an officer to generally oversee or enforce compliance with its provisions. It is submitted that the establishment of an organ for the specific purpose of overseeing the working of the Privacy Act and providing support for individuals in obtaining a hearing and appropriate redress will ensure compliance⁹⁹² with the Act and enhance its overall enforcement.

⁹⁸⁷ Section 552a(a)(2); see *Raven v Panama Canal Co* 583 F 2d 169 (5th Cir. 1978).

⁹⁸⁸ *St Michael's Convalescent Hospital v California* 643 F.2d, 1369, 1373 (9th Cir. 1981); *Dresser Industries v United States* 596 F.2d 1231 (5th Cir. 1979).

⁹⁸⁹ (No 98-2523) (DDC Jan 31, 2002).

⁹⁹⁰ Public Law 100-503 The Computer Matching and Privacy Protection Act of 1988. See below Para 3.3.3.1.3.

⁹⁹¹ The Computer Matching and Privacy Protection Act of 1988 as amended in 1991.

⁹⁹² Cf P Birkinshaw *Freedom of Information: The Law, the Practice and the Ideal* (2001) at 62.

4.3.1.1a Relevance to Internet Cafes

Internet cafes are not government agencies but privately owned businesses and to this extent, the provisions of the Privacy Act will not be directly applicable to the practice in Internet cafes. However, the adoption of two basic principles included in the Privacy Act will be beneficial useful for the protection of privacy in Internet cafes. These are: the principle whereby the public is allowed to know what information regarding them is being kept and, the principle that data should only be processed in accordance with the purpose for which it was obtained. These principles are also contained in the OECD principles.

4.3.1.1.2 Freedom of Information Act⁹⁹³

The Privacy Act and the Freedom of Information Act are complementary.⁹⁹⁴ Both statutes are directly applicable to Federal agencies as well as other independent agencies that process or control the flow of information.⁹⁹⁵ The Freedom of Information Act governs public access to all records maintained by the Federal Government. The Act was enacted in 1966 to promote public access to information in the possession of the Federal Government and it has been subsequently amended.⁹⁹⁶ Each state has its own public

⁹⁹³ (1966) 5 USC Section 552 as amended in 1974 and 1986.

⁹⁹⁴ Cf Birkinshaw op cit at 61.

⁹⁹⁵ Section 552(f)(1).

⁹⁹⁶ 1974, 1986.

access to information laws that need to be consulted for access to state and local records.⁹⁹⁷

The main objective of the Freedom of Information Act is disclosure of government records. The first part of the Act provides procedural rules for government agencies that collect information.⁹⁹⁸ It prescribes that agencies must make information available to the public regarding the agencies,⁹⁹⁹ persons from whom, and methods by which information, or decisions may be obtained, or “submittals” and requests made.¹⁰⁰⁰

The Act also provides that agencies must make certain information available for public inspection and copying.¹⁰⁰¹ These include final opinions and orders made in the adjudication of cases,¹⁰⁰² administrative staff manuals and instructions to staff which affect members of the public,¹⁰⁰³ as well as copies of all records that have been made available to any person, under certain circumstances.¹⁰⁰⁴ Although these provisions primarily regulate disclosure (and collection) of information, they also serve as a form of check on both the powers and the activities of such agencies in disclosing information. These provisions are useful in an indirect manner to protect privacy.

⁹⁹⁷ Cf Banisar & Davies *op cit*; Sloan *op cit* at 17f.

⁹⁹⁸ Section 552 (a)(1)-(6).

⁹⁹⁹ Section 552 (a)(1)(A)-(E).

¹⁰⁰⁰ Section 552(a)(1)(A).

¹⁰⁰¹ Section 552(a)(2).

¹⁰⁰² Section 552(a)(2)(A).

¹⁰⁰³ Section 552(a)(2)(C)

¹⁰⁰⁴ Section 552 (a)(2)(D) and (E).

The Act contains other provisions that protect privacy more directly. Notable among these is the provision specifying that identifying details may be deleted from policy statements, opinions, interpretations, staff manuals and instructions, as well as copies of records “to the extent required to prevent a clearly unwarranted invasion of personal privacy”.¹⁰⁰⁵

There are nine significant exemptions from the general rule requiring disclosure of any reasonably described records to protect individual privacy interests. Among the exemptions are “trade secrets, and commercial or financial information obtained from a person and privileged or confidential” information;¹⁰⁰⁶ “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy”;¹⁰⁰⁷ records or information compiled for law enforcement purposes, where the production of such records might constitute an invasion of privacy, violate the confidentiality rights of the State, private institutions or persons, or in other ways jeopardise the interest of the law, private persons or the State;¹⁰⁰⁸ and, certain kinds of financial records.¹⁰⁰⁹

¹⁰⁰⁵ Section 552(a)(2)(E).

¹⁰⁰⁶ Section 552(b)(4). See *Critical Mass Energy Project v NRC* 975 F.2d 871 (Dc Cir. 1992); (1993) 113 SCt 1579.

¹⁰⁰⁷ Section 552(b)(6). In *Wine Hobby v I. R. S.* 502 F.2d 133 (3d Cir. 1974), the court refused to order the disclosure of the names and addresses of people who had registered as home wine-makers in accordance with tax-law requirements, when the request was made so that the manufacturer could send them advertisements.

¹⁰⁰⁸ Section 552(b)(7)(A)-(F). See *N.L.R.B. v Robbins Tire & Rubber Co.* (1978) 98 SCt 2311; *Maroscia v Levy* 569 F.2d 100 (7th Cir. 1977), where it was established that the identity of confidential informants in

In *Department of Justice v Reporters Committee for Freedom of the Press*,¹⁰¹⁰ the Department of Justice's denial of disclosure of certain criminal records concerning members of the Medico family on the basis of one of the exemptions¹⁰¹¹ was upheld. In this case, the court established that the purpose of the Freedom of Information Act is to ensure openness in the Government's activities, and not the disclosure of government-held information about private citizens.¹⁰¹²

Other categories of information protected under the exemptions in the Freedom of Information Act include matters authorised, and or classified by virtue of an Executive Order to be kept secret in the interests of national defence or foreign policy;¹⁰¹³ matters related to the internal personnel rules and practices of agencies;¹⁰¹⁴ under certain circumstances, matters exempted from disclosure by statute;¹⁰¹⁵ inter-agency and intra-agency memorandums;¹⁰¹⁶ and, letters that are not ordinarily available to members of the public.¹⁰¹⁷

criminal or national security investigations, as well as any information that may threaten the safety of those involved, may be withheld. See also *U.S. Dept of Justice v Landano* (1993) 113 SCt 2014.

¹⁰⁰⁹ Section 552(b)(8).

¹⁰¹⁰ (1989) 489 US 749.

¹⁰¹¹ Exemption (7)(c).

¹⁰¹² At 774.

¹⁰¹³ Section 552(b)(1).

¹⁰¹⁴ Section 552(b)(2). See *Petroleum Info Corp v U.S. Dept of Int.* (1992) 976 F 2d 1429; *Quarles v Dept of Justice* (1990) 890 F 2d 390; *Wolfe v HHS* (1988) 839 F 2d 768.

¹⁰¹⁵ Section 552(b)(3).

¹⁰¹⁶ Section 552(b)(4).

¹⁰¹⁷ Section 552b(5).

It has however been established that reliance on an exemption by an agency is discretionary, therefore, information that is exempt under the Act may still be disclosed.¹⁰¹⁸ It is submitted that to the extent that the rights provided for under the Act are discretionary, those rights cannot be regarded as guaranteed rights, neither can an individual be certain of or rely on their protection in this regard.

With regard to enforcement of the Act, there is no public official - ombudsman, commissioner or registrar- to ensure compliance with the rules and procedure laid down in the Act. There is however the Office of Special Counsel which oversees compliance with specific aspects of the Act and also performs certain duties of an ombudsman.¹⁰¹⁹

The Electronic Freedom of Information Act of 1996¹⁰²⁰ has amended the Freedom of Information Act of 1966¹⁰²¹ by extending the provisions of the Freedom of Information Act regarding disclosures to computerised records. In essence, the Act requires that records maintained in electronic format must be made accessible in the same way as paper records.¹⁰²²

¹⁰¹⁸ *Chrysler Corpn. v Brown* (1979) 99 SCt 1705.

¹⁰¹⁹ For instance, the Special Counsel are empowered to require agencies to respond to all allegations and to initiate disciplinary action against officials who abuse their powers. See N Marsh *Public Access to Government-Held Information* (1987) at 82-3.

¹⁰²⁰ Public Law 104-231, 110 Stat 3048, 1996.

¹⁰²¹ 5 USC Section 552.

¹⁰²² 5 USC Section 552(f)(2).

4.3.1.2a Relevance to Internet Cafes

As in the case of the Privacy Act, the provisions of the Freedom of Information Act are not directly relevant for the protection of information processed in Internet cafes. However, the following principles from the Freedom of Information Act should be considered and adapted in any law for general data protection and/or privacy and data protection in Internet cafes in Nigeria: The right to know that personal information is being kept and by whom; the right of access to such data; the regulation of the use and the disclosure of such information, and the authority to influence, (by correcting or deleting inaccurate) such data. These principles are enumerated in the European Union Data Protection Directive¹⁰²³ and contained in the United Kingdom Data Protection Act.¹⁰²⁴

4.3.1.3 Computer Matching and Privacy Protection Act 1988¹⁰²⁵

The Computer Matching and Privacy Protection Act regulates computer matching of Federal data for verifying eligibility for Federal benefits programmes or for recouping delinquent debts. The Act requires that agencies involved in computer matching programs develop policies and procedures that must be approved by an Agency Data

¹⁰²³ The European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data. 95/46/EC/1995. Cf above Para 3.2.3.2.1.

¹⁰²⁴ Cap 29 of 1988. Cf above Para 3.2.3.2.2.5.

¹⁰²⁵ (1988) 5 USC Section 552a, Public Law 101-56 July 19 1989.

Integrity Board.¹⁰²⁶ It also requires that agencies using records obtained through a matching programme must verify that the information provided is accurate before taking any action that will affect an individual adversely,¹⁰²⁷ and that individuals must be given a chance to respond before such agencies take action.¹⁰²⁸

4.3.1.3a Relevance to Internet Cafes

Again, this provision will not be of much relevance for the protection of privacy in Internet cafes. Since Internet cafes are set up primarily to provide Internet and other computer-based services to consumers, any use of information outside the purview of this purpose should be restricted. It is submitted that unless they are properly licensed or authorized so to do, computer matching between computers in an Internet café and/or other computers should be outlawed.

4.3.1.4 Right to Financial Privacy Act 1978¹⁰²⁹

The Right to Financial Privacy Act lays down strict procedures by Federal agencies regarding the scanning customer records.¹⁰³⁰ Under the Act, it is illegal for government

¹⁰²⁶ Section 552a(U)(1).

¹⁰²⁷ Section 552a(P)(1)(A).

¹⁰²⁸ Section 552a (P)(1)(B).

¹⁰²⁹ (1978) 12 USC Section 3401 et seq, Public Law 95-630.

¹⁰³⁰ Section 3402.

authorities¹⁰³¹ to access records pertaining to customers' relationships with consumer reporting agencies, credit card companies and other financial institutions,¹⁰³² except in compliance with the provisions of the Act.¹⁰³³ The Act prohibits the release of financial records by financial institutions unless done in accordance with its provisions.¹⁰³⁴ It also provides that customers must authorise the disclosure of financial records pertaining to them and regulates such authorisations.¹⁰³⁵

4.3.1.4a Relevance to Internet Cafes

This is another subject-specific Act that will not bear any direct relevance to the protection of information processed in Internet cafes except to underline the highly confidential nature of financial information and suggest strict laws to regulate access and disclosure thereof.

4.3.1.5 Fair Credit Reporting Act 1970¹⁰³⁶

¹⁰³¹ This includes agencies, departments, officers, employees or agents of the United States. (Section 3401 (3)).

¹⁰³² Section 3401(1) & (2).

¹⁰³³ Section 3402.

¹⁰³⁴ Section 3403.

¹⁰³⁵ Section 3404.

¹⁰³⁶ (1970) 15 USC Section 1681 amended in 1992; See also Fair Credit Reporting Act, Public Law 91-508, amended by Public Law 104-208, (Sept 30,1996).

The Fair Credit Reporting Act prohibits the disclosure of credit information by organisations involved in obtaining information where such disclosure is not for any of the permissible purposes described under the Act.¹⁰³⁷ Some of these permissible purposes include, providing information directly to the individual named in the report;¹⁰³⁸ providing information in instances where in business, there is a legitimate need to disclose such information, (for instance, where a person is applying for credit or insurance);¹⁰³⁹ and providing information in response to a court order.¹⁰⁴⁰

The Act prohibits the procurement of investigative consumer reports on consumers not made in compliance with procedure specified under the Act,¹⁰⁴¹ which includes disclosure to the consumer of the fact,¹⁰⁴² as well as the nature and scope of the investigation.¹⁰⁴³ The Act also provides that consumers have the right of access to all information maintained by a consumer reporting agency in the their file at the time of requesting¹⁰⁴⁴ and to know the sources, (except investigative sources) of such information.¹⁰⁴⁵

¹⁰³⁷ Section 1681(b).

¹⁰³⁸ Section 1681(b)(a)(2).

¹⁰³⁹ Section 1681(b)(a)(3).

¹⁰⁴⁰ Section 1681(b)(a)(1).

¹⁰⁴¹ Section 1681(d).

¹⁰⁴² Section 1681(d)(a).

¹⁰⁴³ Section 1681(d) (b).

¹⁰⁴⁴ Section 1681(g)(a)(1).

¹⁰⁴⁵ Section 1681(g)(a)(2).

The Act also gives consumers the opportunity to correct errors in their credit files.¹⁰⁴⁶ These provisions protect the right to privacy by allowing the consumer to be aware of information available about him or her and to exercise some measure of control over the information. Section 1681c of the Act provides for the exclusion of certain information¹⁰⁴⁷ from consumer reports.

4.3.1.5a Relevance to Internet Cafes

The Fair Credit Reporting Act regulates the procedure of credit reporting agencies and is not directly relevant for the protection of information processed in Internet cafes.

4.3.1.6 Electronic Funds Transfer Act 1978¹⁰⁴⁸

The Electronic Funds Transfer Act regulates the use of electronic banking systems such as point-of-sale terminal, telephone bill payments, automated teller machine (ATM), and others.¹⁰⁴⁹ The Act requires that institutions inform their customers about circumstances in which information will be disclosed to a third party in the ordinary course of business.¹⁰⁵⁰ Knowledge that information regarding them may be held by third parties

¹⁰⁴⁶ Section 1861(i).

¹⁰⁴⁷ These include information relating to civil suits, judgements and records of arrest which “from the date of entry antedate the report by more than seven years”, and “paid tax liens which, from the date of payment, antedate the report for more than seven years” and other specified information.

¹⁰⁴⁸ (1978) 15 USC Sections 1693-1693r.

¹⁰⁴⁹ Section 1693(a)(6).

affords customers the opportunity to proceed with or recede from the intended transactions, or to take proper precautionary measures (where possible) for the protection of their privacy.

The Act also regulates the issue of codes and other means of access to accounts.¹⁰⁵¹ It prohibits the issuing of credit or ATM cards, codes and other means of access to consumers for the purpose of accessing their accounts, except in response to a request or application for such¹⁰⁵² and as replacements or renewals for existing cards.¹⁰⁵³ The Act's regulation of access to accounts provides a measure of security against fraudulent invasions of privacy.

4.3.1.6a Relevance to Internet Cafes

This Act is not directly relevant for the protection of privacy and data in Internet cafes as it primarily establishes guidelines and procedures for banking service providers to follow in order to safeguard clients' privacy. However, the provisions of the EFTA when complied with will also protect the privacy of customers where electronic banking is done at an Internet café.

¹⁰⁵⁰ Section 1693(c)(9).

¹⁰⁵¹ Section 1693(i).

¹⁰⁵² Section 1693(i)(a)(1)

¹⁰⁵³ Section 1693(i)(a)(2).

4.3.1.7 Children's Online Privacy Protection Act (COPPA) 1990 ¹⁰⁵⁴

The Children's Online Privacy Protection Act requires commercial website operators to provide clear notice of their information-gathering practices¹⁰⁵⁵ and obtain prior parental consent when eliciting personal information from children under 13 years of age.¹⁰⁵⁶ The Act also allows parents to access and check information that has been collected¹⁰⁵⁷ and to curtail its use.¹⁰⁵⁸ The Act also requires website operators "to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children".¹⁰⁵⁹

4.3.1.7a Relevance to Internet Cafes

This Act will be relevant for the protection of privacy and data in Internet cafes where an Internet café also operates a commercial website. In such cases, the Internet café will be required to notify clients of their information-gathering practices and to protect the confidentiality of information gathered. It is also suggested that the adoption of a provision requiring the obtaining of parental consent prior to the eliciting of personal information from children under 13 years of age when using Internet café facilities in

¹⁰⁵⁴ 15 USC Sections 6501- 6506.

¹⁰⁵⁵ Section 6502(b)(i).

¹⁰⁵⁶ Section 6502(b)(ii).

¹⁰⁵⁷ Section 6502(B)(i) & (iii).

¹⁰⁵⁸ Section 6502(B)(ii).

¹⁰⁵⁹ Section 6502(D).

Nigeria will be beneficial for the protection of children's privacy in Nigeria. It is further suggested that, as provided for in the COPPA, such information should be accessible to parents and parents should be able to exercise some control over its use.

4.3.1.8 Video Privacy Protection Act 1988¹⁰⁶⁰

The Video Privacy Protection Act forbids those who sell or rent videos from disclosing personal identifiable information about their customers.¹⁰⁶¹ The Act also forbids the disclosure of customers' selections.¹⁰⁶²

4.3.1.8a Relevance to Internet Cafes

This Act will be relevant where video rental services are also included in the business of an Internet café. In such a case, the Internet café personnel will be prohibited from disclosing personal identifiable information about their customers or/and about their customers selections.

4.3.1.9 Family Educational Rights and Privacy Act 1974¹⁰⁶³

¹⁰⁶⁰ (1988) 18 USC Section 2710.

¹⁰⁶¹ Section 2710(b)(1).

¹⁰⁶² Section 2710(b)(2)(D)(ii).

¹⁰⁶³ (1974) 20 USC Section 1232g; Public Law 93-380.

The Family Educational Rights and Privacy Act (FERPA), restricts the disclosure of school records to persons other than the parents or students themselves.¹⁰⁶⁴ The Act however makes exceptions in favour of state educational authorities as well as Federal and local authorities in the exercise of their lawful duties.¹⁰⁶⁵ The United States of America PATRIOT Act of 2001¹⁰⁶⁶ amended the FERPA in 1994 to permit disclosure of records relating to the investigation and prosecution of terrorism to the appropriate Federal authorities.¹⁰⁶⁷ It is submitted that this, as well as other provisions of the PATRIOT Act, undermines the right to privacy and data protection recognised in the Amendments to the United States Constitution.¹⁰⁶⁸

4.3.1.9a Relevance to Internet Cafes

This Act will only be relevant to the protection of privacy and data in Internet cafes where school records are disclosed through an Internet café.

4.3.1.10 Drivers' Privacy Protection Act 1994¹⁰⁶⁹

¹⁰⁶⁴ Section 1(A), Section 2.

¹⁰⁶⁵ Paragraphs 3, 4(a) & 5.

¹⁰⁶⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001; Public Law 107-56; 115 Stat. 272. Cf below Para 4.3.1.13.

¹⁰⁶⁷ Section 507.

¹⁰⁶⁸ Cf above Para 3.3.1.1ff.

¹⁰⁶⁹ (1994) 18 USC Section 2721 et seq, Public Law 103-322.

The Drivers' Privacy Protection Act prohibits the release and use of certain personal information. Specifically, it prohibits state "Departments of Motor Vehicles" (DMV's) from releasing personal information about license holders.¹⁰⁷⁰ The Act protects privacy by restricting access to personal information through state motor vehicle agencies.¹⁰⁷¹ The Act however permits disclosure of personal information where such information is to be used in relation to matters of motor vehicle or driver safety, performance monitoring, and other specified matters relating to motor vehicles.¹⁰⁷²

The Act also makes exceptions to the provision prohibiting disclosure in specific instances.¹⁰⁷³ These include information required by Federal, state and local agencies,¹⁰⁷⁴ legitimate businesses and their agents, employees or contractors¹⁰⁷⁵ for purposes related to motor vehicle or driver safety or any of the purposes specified in the Act,¹⁰⁷⁶ or to verify the accuracy of personal information submitted to them.¹⁰⁷⁷ It has been observed that these exceptions are wide and that "anyone who is willing to pay" may be able to obtain information under subsection b of section 2721 (the Act).¹⁰⁷⁸

¹⁰⁷⁰ Section 2721 (a)(1) & (2).

¹⁰⁷¹ *Reno v Condon* (2000) 528 US 141.

¹⁰⁷² Section 2721(b).

¹⁰⁷³ Section 2721(a)(1) to (14).

¹⁰⁷⁴ Section 2721(b)(1).

¹⁰⁷⁵ Section 2721(b)(3).

¹⁰⁷⁶ Section 2721(b)(2).

¹⁰⁷⁷ Section 2721(b)(3).

4.3.1.10a Relevance to Internet Cafes

The Drivers' Privacy Protection Act applies to state "Departments of Motor Vehicles" (DMV's). Its provisions will only be relevant for the protection of privacy and/or data in Internet cafes where persona information relating to a license holder is processed or disclosed via an Internet café.

4.3.1.11 Wiretap Act 1968¹⁰⁷⁹

The Wiretap Act regulates the interception of telephone communications. The decision in *Katz v Olmstead*¹⁰⁸⁰ was codified as the Wiretap Act of 1968. In essence, it provides protection against unjustified search and seizure of information traveling on a telephone by prohibiting tapping of telephone lines without a warrant. The Act also establishes the basic requirements for a search warrant in respect of government interception of telephone communications.¹⁰⁸¹ It also makes it illegal for private persons to make recordings of telephone calls without the consent of the parties to the call.¹⁰⁸²

Although the Act protects privacy by prohibiting disclosure of information, it has been held that these prohibitions will not apply to the media when the information to be

¹⁰⁷⁸ H. Henderson *Privacy in the Information Age* (1999) at 43.

¹⁰⁷⁹ 1968 (Title 3 of the Omnibus Crime Control Bill).

¹⁰⁸⁰ *Supra*.

¹⁰⁸¹ Section 2511(2).

¹⁰⁸² Section 2511(2)(d).

published is of public concern.¹⁰⁸³ As previously mentioned,¹⁰⁸⁴ the advancement and increasing sophistication of technology have resulted in amendments to the law on wiretapping.

4.3.1.11a Relevance to Internet Cafes

By virtue of the Wiretap Act, the interception or recording of telephonic conversations in Internet cafes will be prohibited unless it is done in accordance with the provisions of the Act.

4.3.1.12 Electronic Communications Privacy Act 1986¹⁰⁸⁵

Following conclusions by the Justice Department that the Wiretap Act did not apply to e-mail and other computer communications, the Electronic Communications Privacy Act of 1986 (ECPA) was passed to extend the protection provided under the Wiretap Act to electronic mail and computer communications. The ECPA covers voice communication devices such as radio-paging devices and cellular telephones, as well as electronic mail,¹⁰⁸⁶ which are not covered by the Wiretap Act.

¹⁰⁸³ *Bartnicki v Vopper* (2001) 532 US 514, 121 SCt 1753. This decision has however been criticised as erroneous. T Wilkinson "Is Anyone Listening to me? *Bartnicki v Vopper*" 63 *Louisiana Law Review* (2003), Vol 63 No 2 at 601ff.

¹⁰⁸⁴ At Para 4.1.1.3.

¹⁰⁸⁵ 18 USC Section 2510

¹⁰⁸⁶ ECPA 18 USC Section 2511(a).

In *McVeigh v Cohen et al.*,¹⁰⁸⁷ where the defendant had discharged the plaintiff from duty on the basis of information obtained from e-mail, and AOL, an Online Service Provider, without the defendants having complied with the procedure laid down by the ECPA for obtaining information, the court issued an injunction to block the plaintiff's discharge. The ECPA however does not apply to transmissions made over a cordless telephone.¹⁰⁸⁸ The provisions of SS 2511 of the ECPA have been significantly amended by the USA PATRIOT Act 2001.¹⁰⁸⁹

4.3.1.12a Relevance to Internet Cafes

By virtue of the Electronic Communications Privacy Act the protection afforded telephone conversations by prohibiting interception and recording unless done in accordance with laid down procedure will be extended to electronic mail and cellular phone communications in Internet cafes. Thus it will be unlawful to intercept and record e-mail and cellular phone communications transacted in an Internet café unless the relevant provisions of the law are complied with. The ECPA will be relevant for the protection of information whether contained in e-mail or transacted by means of cellular phone in an Internet cafe.

¹⁰⁸⁷ 983 F Supp 215 (D) DC (1998); Cf *Steve Jackson Games Inc v US Secret Service* 816 F Supp 432 (W.D. Tex); 36 F 3d 457 (5th Cir. 1994); where the court held that seizure of a computer containing private stored e-mail did not constitute interception under the Act, as the e-mail was not being transmitted when the computer was taken. See also *Davis et al v Gracey et al* No 95-6245 (10th Cir.) 21 April 1997.

¹⁰⁸⁸ Section 2511(a). See also *United States v David Lee Smith* supra.

¹⁰⁸⁹ {Sections 202, 203, 212, 214} Public Law 107-56; 115 Stat 272 (2001); Cf below Para 4.3.1.13.

4.3.1.13 USA PATRIOT Act 2001¹⁰⁹⁰

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001¹⁰⁹¹ creates exceptions to the law on wiretapping. The Act provides authority to intercept wire, oral and electronic communications for the purpose of averting terrorism.¹⁰⁹² “Terrorism” is defined in the Act in terms of domestic¹⁰⁹³ and federal¹⁰⁹⁴ terrorism. Domestic terrorism is defined as:

“[A]ctivities that-

- (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
- (B) appear to be intended-
 - (i) to intimidate or coerce a civilian population;
 - (ii) to influence the policy of a government by intimidation or coercion;
 - (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and

¹⁰⁹⁰ Public Law 107-56; 115 Stat 272 (2001).

¹⁰⁹¹ Public Law 107-56; 115 Stat 272 (2001).

¹⁰⁹² Section 201.

¹⁰⁹³ Section 802.

¹⁰⁹⁴ Section 808.

(C) occur primarily within the territorial jurisdiction of the United States.”¹⁰⁹⁵

The definition of federal terrorism¹⁰⁹⁶ consists of a series of amendments to certain sections of federal law¹⁰⁹⁷ and a long list of specified acts that would amount to federal terrorism.¹⁰⁹⁸

The relevant provisions of the PATRIOT Act affecting the right to privacy amend certain sections of the Electronic Communications Privacy Act (ECPA).¹⁰⁹⁹ Sections 202 and 203 of the PATRIOT Act amend sections 2516 and 2517 of the ECPA. Sections 2516 and 2517 regulate and create exceptions to the rules on the interception, disclosure and use of oral, wire and electronic communications. Section 202 of the PATRIOT Act authorises the interception of wire, oral and electronic communications in matters relating to computer fraud and abuse.¹¹⁰⁰

Section 203 of the PATRIOT Act authorises law enforcement agents to disclose contents of wire, oral and electronic communications to other Federal Intelligence or security officials where such information includes Foreign Intelligence or Counter-intelligence

¹⁰⁹⁵ Section 802(a)(5).

¹⁰⁹⁶ Section 808.

¹⁰⁹⁷ Section 2332(b) of 18 USC.

¹⁰⁹⁸ Section 808(2). Some of these include: destruction of aircraft or aircraft facilities, violence against maritime navigation, use of weapons of mass destruction.

¹⁰⁹⁹ ECPA 18 USC Section 2510 et seq.

¹¹⁰⁰ Section 202.

information. “Foreign Intelligence Information” is defined in the Act to include “information, whether or not concerning a United States person, that relates to the ability of the United States government to protect against actual or potential attack or other grave hostile acts of a foreign power”, or its agent, and “clandestine intelligence activities by an intelligence service or network of a foreign power,” or its agent.¹¹⁰¹

Section 204 deals with clarification of intelligence exceptions from limitations on the interception and disclosure of wire, oral and electronic communications. This amends¹¹⁰² by widening the scope of the former provision to include electronic communications. Section 212 of the PATRIOT Act provides for emergency disclosure of electronic communications to protect life and limb, thus creating further exceptions to the rule forbidding disclosure of electronic communications in section 2511 of the ECPA.

Section 217 of the PATRIOT Act allows the interception of communication carried on by computer trespassers. With regard to data, section 711 of the Act provides for the expansion of regional information sharing system to facilitate the flow of information between federal, state and local law enforcement agents in matters related to terrorism.

As observed above,¹¹⁰³ these provisions allow infringements of the constitutionally recognized right to privacy and together, they greatly detract from the protection available for privacy in the United States.

¹¹⁰¹ Section 203(b)(2).

¹¹⁰² 18 USC Section 2511(2)(f).

Apart from the PATRIOT Act, there are other provisions allowing secret interception or recording of communication with the consent of the parties involved in the communication.¹¹⁰⁴

4.3.1.13a Relevance to Internet Cafes

By virtue of the USA Patriot Act, any communications in any Internet café may be intercepted in matters relating to computer fraud and abuse, for the protection of life and limb, and in the interest of national security without incurring any liability for breach of any laws. It is submitted that although the right to privacy may lawfully be overridden for the protection of other interests, the leeway given by the PATRIOT Act is too broad and there is a need for further qualification to avoid abuse. In this regard, it is submitted that in Nigeria an Act similar to the USA PATRIOT Act would be unconstitutional and void to the extent that its provisions are inconsistent with Section 36 of the Nigerian Constitution.

4.3.1.14 Federal Copyright Law¹¹⁰⁵

Federal copyright law protects literary and artistic property including written words, images, tape-recorded conversations and photographs.¹¹⁰⁶ The law also prohibits

¹¹⁰³ Para 3.3.3.1.9.

¹¹⁰⁴ For instance, 18 USC Section 2511(2)(d).

¹¹⁰⁵ 17 USC Sections 101 et seq; 18 *Am Jur 2d*, Copyright and Literary Property Article 76.

commercial exploitation of another's personality.¹¹⁰⁷ A person has the absolute right to control the commercial use of his or her personality and this covers the use of name, photograph, likeness, voice and identifying slogans.¹¹⁰⁸ Thus in *Midler v Young & Rubicam*,¹¹⁰⁹ where the plaintiff's sound and style as an entertainer was imitated by a vocalist, the plaintiff was awarded damages.

4.3.1.14a Relevance to Internet Cafes

This law will only be relevant for the protection of information processed in Internet cafes where literary or artistic information processed via an Internet café is wrongfully used.

4.3.2 Protection of Privacy and Data under State Laws

There are various state laws protecting privacy and data covering many of the areas for which Federal legislation provides. For instance, state law in Maryland forbids the disclosure of financial records by fiduciary institutions without the authority of the customer, unless the records are subpoenaed.¹¹¹⁰ Similarly in Illinois, banks are

¹¹⁰⁶ Section 102.

¹¹⁰⁷ See sections 102, 106- 1022.

¹¹⁰⁸ Ibid.

¹¹⁰⁹ 849 F2d 460 (9th Cir. 1988), 944 F2d 909 (9th Cir. 1991). See also *White v Samsung Electronics America Inc.* 989 F2d 1512 (9th Cir. 1993), where a robot was used to imitate the plaintiff.

¹¹¹⁰ Md. Ann. Code art. 11, sec.225.

prohibited from disclosing customer information without customer authorisation, a subpoena, a regulatory agency request or credit exchange.¹¹¹¹

There are also state laws governing credit reporting and investigation. In Arizona, for instance, the law states that “the sources of investigative consumer reports must be furnished to the consumer upon request, along with the contents of any report.”¹¹¹² The law further requires the investigative company (or agency) to alter its file in accordance with the consumer’s version, where there is notice of inaccuracy about the facts in the file and these cannot be verified.¹¹¹³

Several states have Information Practice Acts to protect information in government data banks.¹¹¹⁴ The Arkansas Information Practice Act¹¹¹⁵ codifies the principles of fair information practices. These principles include the prohibition of the existence of secret personal information systems as well as the collection of unneeded or irrelevant data and a requirement for enabling citizens to inspect data kept on them.¹¹¹⁶

¹¹¹¹ III. Rev. Sta. Ann.Ch. 161\2, sec.48.1 (Supp.1977).

¹¹¹² Ariz. Rev. Stat. Sec. 44-1693(A)(4).

¹¹¹³ Ibid. See also Cal. Civil Code sec. 1786; Mont. Rev. Codes Ann. Sec. 18-501.

¹¹¹⁴ For instance Arkansas: Ark. Stat. Ann. Sec. 16-804; California: Cal. Civil Code sec. 1798; New Hampshire: N.H.Rev. Stat. Ann. 7-A; Utah: Utah Code Ann. Sec.63-50-1.

¹¹¹⁵ Ark. Stat. Ann. Sec.16-804.

¹¹¹⁶ Section 16-804.

The various state legislatures also make laws that regulate wiretaps and telegraphic communications within the state.¹¹¹⁷ These laws generally provide for circumstances in which it is illegal to intercept telephone and electronic communications, and they also provide penalties for unauthorised interception of communications. In Alabama, the law provides that “Any person who shall intercept, read or in any manner interrupt or delay the sending of a message over any telegraph or telephone line shall be guilty of a misdemeanour.”¹¹¹⁸

In Michigan, the law prohibits eavesdropping on telephone conversations without the consent of both parties to the conversation,¹¹¹⁹ and in Washington State, the interception of electronic communications without the consent of all the parties to the communication is prohibited.¹¹²⁰ In many states however, consent of one of the parties to the conversation is sufficient in order to lawfully monitor such communication.¹¹²¹ There are also state laws that forbid employees of telephone companies from disclosing the contents of telephone communications.¹¹²²

¹¹¹⁷ For instance Alabama: Ala. Code tit 14, sec 84; Alaska: Alaska Stat. Sec. 11.60.290; Maryland: MD. Ann. Code art. 10, sec.401.

¹¹¹⁸ Ala. Code tit 14, sec 84 (18).

¹¹¹⁹ Mich. Comps. Laws Ann. Sec. 750-539.

¹¹²⁰ Washington: RCW 9.73.030.

¹¹²¹ For example Alaska: Alaska Stat. sec. 11.60.290; Maine: Me. Rev. Stat. Tit.15, sec.709. In New Hampshire and some other states, the provisions of the state law are the same as Federal law (18 USC Section 2510), which prohibits interception of wire or oral communication where none of the parties have consented to the interception and lays down exceptions to the general rule. See N.H. Rev. Stat. Ann. sec.570; A1.

4.3.2a Relevance to Internet Cafes

As mentioned above, many of the federal statutes protecting different aspects of privacy and data are replicated at the federal level. However, none of the available laws specifically protects privacy and/data in Internet cafes. The different state laws such as laws governing the interception of communications and credit reporting, will only be relevant to the extent that their provisions bear relevance and are applicable to practices in Internet cafes with respect to access to and disclosure of information.

4. 4 Conclusion on the Law Protecting Privacy and Data in the United States

In the United States, although the Constitution does not specifically guarantee the right to privacy, certain provisions create a limitation on government action for the protection of an individual's privacy,¹¹²³ and the courts have accordingly interpreted these provisions to guarantee privacy in various circumstances. Moreover, the presence of both Federal laws and state laws protecting privacy and data creates greater awareness of the laws and ensures better administration in terms of enforcement of these laws at all levels.

In addition to the constitutional recognition of the right to privacy, the Common Law confers personal rights on individuals against other individuals or group of persons, including juristic persons where applicable.¹¹²⁴ Based on the unequivocal constitutional

¹¹²² Mich. Comps. Laws Ann. Sec. 750-539.

¹¹²³ See generally *Griswold v Connecticut* (1965) US 479 at 484, 85 SCt 564. See above at para 3.3.1.1ff.

and Common Law recognition and development of a right to privacy, and the (generous) availability of statutes at both Federal and state levels for the protection of privacy, it may be asserted that the law protecting privacy is clear, well-defined, and better developed in the United States, than in the United Kingdom.

However, although the principles developed from the cases against the background of the Constitution give the protection of the right to privacy a firm footing in the United States, there are many loopholes in the American law of privacy. For instance, it has been said¹¹²⁵ that for a right to be affirmed by the American courts, it must be deeply rooted in the nation's history and tradition. This places a limitation on the scope of the right to privacy and has sometimes resulted in a narrow understanding of the concept of privacy in the United States.¹¹²⁶

Other decisions of the Supreme Court have been criticised¹¹²⁷ including, the decision based on the Fourth Amendment, that no warrant was required for a telephone company, at the request of law-enforcement officials, to electronically monitor numbers dialed from

¹¹²⁴ See *Dietemann v Time Inc.* supra,

¹¹²⁵ Du Plessis & de Ville in Van Wyk et al op cit at 243.

¹¹²⁶ See *Bowers v Hardwick* (1986) 478 US 186, L Ed 2d 140, 146, 106 SCt 2481, where it was held that the Constitutional right to privacy does not extend to, or give consenting adults the right to engage in acts of sodomy. This decision has however been overruled in *Lawrence v State of Texas* (2003) 539 US 558. Cf also S.A position in *National Coalition for Gay and Lesbian Equality & Others v Minister of Justice & Others* 1998 (6) BCLR 726 (W), 1998 (2) SACR 102 (W). In this case, section 20A(1) of the Sexual Offences Act was declared to be inconsistent with section 8 of the Interim Constitution and invalid because it discriminated against men in general and homosexual men in particular. See also *Case & anor v Minister of Safety and Security & others* 1996 (3) SA 617 where the Constitutional Court held that the prohibition of the use of pornography in the home was an unconstitutional limitation of the right to privacy.

¹¹²⁷ See McQuoid-Mason in Chaskalson et al op cit at 18-13, See also du Plessis & de Ville in van Wyk et al op cit at 245.

a private telephone.¹¹²⁸ As for the Common Law, as observed above,¹¹²⁹ American tort law protection of privacy and data is very limited¹¹³⁰ and, because of the scantiness of successful cases in the area of invasion of privacy in American tort law,¹¹³¹ it has been suggested that the remedy afforded by the courts for invasion of personal privacy is largely illusory.¹¹³²

Concerning statutory protection of privacy, in spite of the abundance of statute law protecting privacy in the United States, these laws have limitations. The provisions of the American Federal Privacy Act¹¹³³ only affords protection for personal information handled by government organisations and employees in Federal agency files.¹¹³⁴ It does not provide a general remedy for disclosure of private information. It has been observed that the Act's failure to provide a general remedy leaves a *lacuna*, with regard to the use of information that is illegally revealed, for example, by the media and other non-governmental parties who may be in a position to disclose information given to them.¹¹³⁵

¹¹²⁸ *Smith v Maryland* supra.

¹¹²⁹ Para 4.2.1.

¹¹³⁰ Cf Roos op cit at 33- 37, where she observes that:

“Prosser’s and the Restatement’s division of the privacy tort into four categories ... have stultified any further development of the privacy tort that could have allowed for coverage of an invasion of privacy by the misuse of data.” (at 37).

¹¹³¹ Cf Anderson in Markesinis op cit at 136ff. Cf also above Para 4.2.1.

¹¹³² See Anderson in Markesinis op cit at 138ff. See also B S Markesinis *The German Law of Torts* (1990) at 322 ff.

¹¹³³ (1974) 5 USC Section 552a.

¹¹³⁴ Section 552e. Cf Marsh op cit at 74.

In addition, as observed above,¹¹³⁶ the provisions of the Privacy Act are often interpreted restrictively, resulting in a limitation of possible protection under the Act. In addition, it is submitted that the failure of the Privacy Act to provide for an official - ombudsman, commissioner or registrar- to ensure compliance with the rules and procedure laid down in the Act detracts from its force.

As for the Freedom of Information Act,¹¹³⁷ the provisions regarding the deletion of identifying details from certain documents or publications in order to prevent a “clearly unwarranted invasion of personal privacy”¹¹³⁸ protect the right to privacy. However, the primary purpose of the Act is to promote access to information. As such, the Freedom of Information Act does not expressly forbid the disclosure of information;¹¹³⁹ it merely regulates disclosure of information.

Furthermore, although the Act provides protection in respect of the information specified in the exceptions,¹¹⁴⁰ the protection provided is limited. Disclosure of information relating to such details is allowed under the Act, and it further provides that under certain circumstances, the amount of information deleted must be indicated in the record that is

¹¹³⁵ Cf Marsh op cit at 84.

¹¹³⁶ At Para 4.3.1.1.

¹¹³⁷ (1966) 5 USC 552 as amended.

¹¹³⁸ Section 552(a)(2)(E).

¹¹³⁹ Section 552d. See also *Chrysler Corporation v Brown* 99 (1979) SCt 1795.

¹¹⁴⁰ Section 552b(1)-(9).

made available, and if technically feasible, at the place in the record where the deletion is made.¹¹⁴¹

It has also been pointed out that the Act leaves a *lacuna* with regard to persons seeking disclosure of information under the Act, as well as the use to which such information is put. In this regard it has been said that the fact that the Act does not make it a requirement for persons seeking access to information to be interested parties, coupled with the fact that once information is gained, it may be used as the party pleases, results in a situation where “it is difficult to say with accuracy who is really seeking the information and what is done with it.”¹¹⁴² To this extent, it may also be said that the Act fails to provide adequate protection for privacy, as there is greater latitude for third parties to access and misuse information. Further to this, the scope of application of the Act is limited in that it applies only to natural persons.¹¹⁴³

As for the other statutes, the protection guaranteed under them will be limited in terms of their specific subject matter and other restrictions that may apply in seeking protection under those statutes. In addition, the fact that these statutes are contained in different documents which are amended from time to time makes access to the laws somewhat tedious.

¹¹⁴¹ Section 552b. See also Anderson in Markesinis op cit at 154-5.

¹¹⁴² See Marsh op cit at 84.

Lastly, the more recent PATRIOT Act¹¹⁴⁴ creates a number of exceptions to the available law regulating and prohibiting the interception of wire, oral and electronic communications in the United States,¹¹⁴⁵ and thus, limits considerably the protection offered against governmental invasions of privacy.

In sum, in spite of the fact that there is a general body of laws in place for the protection of privacy in the United States, there is a *lacuna* in terms of the actual enforcement of these laws, and judiciary interpretation, which has not always favoured the most generous construction for the enjoyment of privacy. The result is that the protection available for data in the United States of America is considerably limited.

4.4a Relevance to Internet Cafes

In extracting principles for the protection of privacy and data generally in Internet cafes, the following is relevant:

The development of the American Constitutional right to privacy in a piecemeal manner creates some difficulty in formulating a unified principle to be followed, thus specific principles will have to be extracted. In this regard, it is submitted that the Fourth Amendment standard of “reasonable expectation of privacy”, as expounded in *Silverman*

¹¹⁴³ Section 552a(a)(2). See also *St Michael's Convalescent Hospital v California* supra; *Dresser Industries v United States* supra.

¹¹⁴⁴ Public Law 107-56; 115 Stat 272 (2001).

¹¹⁴⁵ Cf above Para 4.3.1.13.

*v United States*¹¹⁴⁶ will be a useful yardstick for generally determining whether or not a right to privacy should be recognized in any given case.¹¹⁴⁷

The “reasonable expectation of privacy” standard is relatively malleable, as its application requires consideration of the context and individual circumstances of the plaintiff in each case.¹¹⁴⁸ It is submitted that, considering the fluid nature of the right to privacy¹¹⁴⁹ and the vast potential for infringement,¹¹⁵⁰ such flexibility is necessary for the achievement of fairness from case to case, and it allows the recognition of genuine novel or different-type claims of infringements on privacy rights.

Regarding the Constitutional Amendments it may be said generally that the overall positive construction by the courts¹¹⁵¹ of the provisions of the First,¹¹⁵² Ninth¹¹⁵³ and

¹¹⁴⁶ *Supra*. Cf above Para 4.1.1.3.

¹¹⁴⁷ *Contra* Roos *op cit* at 43, who, on the basis of the decisions in *U.S. v Miller supra* and *Smith v Maryland supra* concludes that “the Fourth Amendment’s “reasonable expectation of privacy” approach makes it unsuitable for protecting privacy in the information age.” It is submitted that those decisions were erroneously reached, and that, correct and appropriate application of the reasonable expectation of privacy criterion will yield positive results for the protection of privacy. Cf the South African courts’ use of the reasonable expectation of privacy criterion above at Para 6.1.

¹¹⁴⁸ *Contra* the tort law requirement of “offensiveness to the *ordinary reasonable person*” used in determining liability for certain torts above at 4.2.1.

¹¹⁴⁹ Cf above Para 1.1.

¹¹⁵⁰ Cf above Para 1.2.

¹¹⁵¹ *Contra* the attitude of the courts towards the development of a Common Law right to privacy in the United Kingdom, above at 3.2.1.1, and in Nigeria, Constitutional protection of privacy, below at 5.2.1.1.

¹¹⁵² Cf above Para 4.1.1.1.

¹¹⁵³ Cf above Para 4.1.1.5.

Fourteenth¹¹⁵⁴ Amendments to accommodate the protection of different acts amounting to invasion of privacy, will be instructive in the interpretation and development of a Nigerian Internet café privacy and/or data protection law. The Third,¹¹⁵⁵ and Fifth¹¹⁵⁶ Amendments provide for specific aspects of the right to privacy and the principles enunciated in them are related to the specified aspects of privacy. Their utility for Nigerian purposes will thus be, to serve as persuasive precedents regarding similar Nigerian provisions. The Third Amendment will also be instructive in establishing a general standard for the processing of information in Internet cafes in accordance with the Nigerian Constitutional right to privacy and other relevant laws.

Although there are many valuable principles in the United States privacy laws, it may be asserted from the preceding that in general, statute law does not solve the current privacy problem posed by Internet collection, disclosure and use of personal identifiable information, especially by private persons.¹¹⁵⁷

As for the Common Law, it is submitted that Prosser's categorisation of the interests protected by the right to privacy will be useful in identifying and grouping cases of invasion of privacy in Nigeria,¹¹⁵⁸ and could be adopted. However, in adopting Prosser's

¹¹⁵⁴ Cf above Para 4.1.1.6.

¹¹⁵⁵ Cf above Para 4.1.1.2.

¹¹⁵⁶ Cf above Para 4.1.1.4.

¹¹⁵⁷ Cf S Byers "The Internet: Privacy Lost, Identities Stolen" (2001-02) 40 *Brandeis Law Journal* 141 at 154.

¹¹⁵⁸ Contra Roos op cit at 33ff, where the utility of Prosser's categorisation for protecting personal privacy is questioned. For our purposes, Prosser's categorisation is useful as a foundation for, and represents an

categorisation, care must be taken not to stifle development of the law by adhering rigidly to the notion that privacy interests are limited to the identified four and rejecting legitimate privacy claims which may not fit perfectly into one of these categories. Thus in suggesting principles for the protection of information processed in Internet cafes in Nigeria, while ensuring that protection for the categories of invasions identified by Prosser is provided for, Prosser's categorisation of interests should not be a closed list.

In Sum, it may be asserted that although not wholly applicable, nor flawless, (certain aspects of) the American privacy law offer(s) relevant and valuable principles for the protection of information processed in Internet cafes in Nigeria.

CHAPTER FIVE

PROTECTION OF PRIVACY AND DATA IN GERMANY

As in the case of the United Kingdom and the United States, the provisions of relevant German laws will be examined with the aim of extracting principles for the protection of electronic mail in Internet cafes, or/and, establishing general guiding principles for the protection of privacy and data in Nigeria.

5.1 Constitutional Protection of Privacy and Data

5.1.1 Constitutional Protection of Privacy

The German Basic Law¹¹⁵⁹ does not make express provision for a general right to privacy, but it makes isolated provision for certain aspects of privacy.¹¹⁶⁰ There is also no express provision on data protection in the Constitution. The protection of a general right to privacy has however been developed by the Federal Constitutional Court on a case-by-case basis.¹¹⁶¹ With respect to data protection, the courts have formally acknowledged an individual's right to informational self-determination, derived from Article 2 of the

¹¹⁵⁹ Basic Law for the Federal Republic of Germany: Basic Rights (1949), as amended by Act of 20 October 1997.

¹¹⁶⁰ See Ackermann J in *Bernstein v Bester* NO 1996 (2) SA 751 (CC) at 793 Para77.

¹¹⁶¹ *Ibid.*

German Basic Law.¹¹⁶² Articles 1 and 2 of the Federal Constitution of 1949 provide for the protection of personality rights.

Article 1(1) states that:

“The dignity of man shall be inviolable. To respect and protect it shall be the duty of all state authority”.¹¹⁶³

Article 2 (1) provides that:

“Everyone shall have the right to the free development of his [or her] personality in so far as he [or she] does not violate the rights of others or offend against the constitutional order or the moral code.”¹¹⁶⁴

Article 2 (2) provides in part that:

“Everyone shall have the right to ... inviolability of his [or her] person. The liberty of the individual shall be inviolable.”

Article 2 also guarantees the right to physical integrity and liberty and it has been said that Articles 1 and 2 of the German Constitution together “guarantee for the individual an

¹¹⁶² 65 *BVerfGE* 1 (1983); See below Para 3.4.1.1.1.

¹¹⁶³ Translation in B S Markesinis *German Law of Torts* (1990) at 288.

inviolable sphere of privacy beyond the reach of public authority.”¹¹⁶⁵ These two provisions were greatly instrumental in the German courts’ development, recognition and protection of the right to privacy.¹¹⁶⁶

In addition to these provisions, Article 10 provides for the privacy of letters, posts and telecommunications¹¹⁶⁷ and Article 13 makes provision for the inviolability of the home.¹¹⁶⁸ These are the major provisions of the German Constitution on the protection of privacy. It is intended to examine case law developments based on these constitutional provisions. Thereafter, comments will be made on their relevance to Internet cafes.

5.1.1.1 The Right to Self- Determination and Protection of Human Dignity

The provisions of Article 1.1 of the Basic Law on the protection of human dignity and Article 2.1 on the right to self-determination are complementary and are often read together by the courts.¹¹⁶⁹ Personality rights include the right of the individual to decide for him- or herself, on the basis of self-determination, when and within what limits, facts

¹¹⁶⁴ Ibid.

¹¹⁶⁵ 1 *BVerfGE* 27 (1969); NJW 1707 (1969); Cf du Plessis & J de Ville “Personal Rights” in D Van Wyk, J Dugard, B de Villiers, & D Davis (eds) *Rights and Constitutionalism: The New South African Legal Order* (1994) at 246.

¹¹⁶⁶ See below. Cf D McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 58.

¹¹⁶⁷ Article 10.

¹¹⁶⁸ Article 13.

¹¹⁶⁹ See generally, for example: 54 *BVerfGE* 208 (1980), 35 *BVerfGE* 202 (1973); Cf D P Kommers *The Constitutional Jurisprudence of the Federal Republic of Germany* 2nd ed. (1997) at 289. See also du Plessis & de Ville op cit at 245 & 6, Markesinis op cit at 301-2.

about his or her personal life should be disclosed.¹¹⁷⁰ The following are aspects of the right to personality that the courts have recognised:

In the *Lebach* case,¹¹⁷¹ the right to determine whether and to what extent others may give a public account of one's life or certain incidents from it was determined. Here, the court held that a German television station would violate the complainant's right to privacy if it broadcast a documentary based on a crime he had committed six years before.

In the *Tape Recording II* case,¹¹⁷² the right to one's own image and spoken word was considered. The court held that a private secret recording made during a discussion to conclude a contract may not be used in criminal proceedings.

In the *Princess Soraya* case,¹¹⁷³ the court held that publication of a fictitious "exclusive" interview with the complainant about her private life revealing intimate details invaded her privacy rights. The right not to have statements falsely attributed to oneself was recognised here.¹¹⁷⁴

¹¹⁷⁰ 1 *BVerfGE* 65, (1941); Cf du Plessis & de Ville op cit at 246.

¹¹⁷¹ 35 *BVerfGE* 202 (1973); *NJW* 1227 (1973).

¹¹⁷² 34 *BVerfGE* 238 (1973); Cf du Plessis & de Ville op cit at 246.

¹¹⁷³ 34 *BVerfGE* 269, 245-51 (1973).

¹¹⁷⁴ Cf Kommers op cit at 322: "It is an infringement of [an individual's] right to privacy to put words into his mouth which he did not utter and which adversely affect his self image."

In the *Klaus K.* case,¹¹⁷⁵ involving the inspection of a letter sent by a wife to her husband, who was being held in pre-trial detention, it was observed that the letter constituted freely written communication to which the courts must attach “special importance” in the light of the constitutional requirement of personal privacy.¹¹⁷⁶ The courts have also, on the basis of Article 2.1, recognised the right to confidentiality with respect to information relating to census¹¹⁷⁷ and legislative investigations.¹¹⁷⁸

Furthermore, in upholding the right to self-determination provided for in Article 2.1, the courts have prohibited general publication of the names of individuals who were no longer allowed to practice as contractual spendthrifts.¹¹⁷⁹ It has also been held that pregnancy belongs to the intimate sphere of a woman and is constitutionally protected by Article 2.1 and Article 1.1¹¹⁸⁰ except where a foetus is aborted.¹¹⁸¹

It must be noted that there are limitations to the enjoyment of the constitutional rights guaranteed in Article 2.1 and Article 1.1. For instance, it has been said, with regard to the constitutional protection of the rights of pregnant women, that the right to privacy does

¹¹⁷⁵ 35 *BVerfGE* 35 (1973).

¹¹⁷⁶ Cf *Kommers op cit* at 576. See also the *Prison Correspondence II* case 35 *BVerfGE* 311 (1973).

¹¹⁷⁷ 65 *BVerfGE* 1, 41-70 (1983).

¹¹⁷⁸ 77 *BVerfGE* 1, 38-63 (1987) (*Neue Heimat*).

¹¹⁷⁹ 78 *BVerfGE* 77, 84-87 (1988).

¹¹⁸⁰ 39 *BVerfGE* 1 (1975) (*Abortion I* case).

¹¹⁸¹ *Ibid.* See also 88 *BVerfGE* 203 (1993) (*Abortion II* case).

not include the right to intrude upon or destroy the protected legal sphere of another, without a justifiable reason, nor does it confer the right to destroy the life itself.¹¹⁸²

In deciding whether or not to uphold a privacy claim, the courts must thus consider the rights accruing to others and strike a just balance between the protection of the private sphere of an individual as against the upholding of other rights of other individuals. The courts must also have regard to the principle of proportionality.¹¹⁸³

In the *Divorce Records*¹¹⁸⁴ case, the court held that the applicant's basic rights protected in Articles 2.1 and 1.1 of the Basic Law were infringed by the decision of the divorce court to hand over recorded evidence of his extra-marital affairs obtained in divorce proceedings to the chief examiner in a disciplinary hearing. According to the court, such an infringement without the consent of the marriage partners could only be justified if it was found to be in accordance with the principle of proportionality.

Accordingly, where an infringement is not in accordance with the principle of proportionality, it will not be justified.¹¹⁸⁵ In the "*Monitoring*" *Opinion*,¹¹⁸⁶ an amendment of Article 10 that would create authority for surveillance contained a part that

¹¹⁸² 39 *BVerfGE* 1 (1975). See also 88 *BVerfGE* 203 (1993) (*Abortion II* case); Cf du Plessis & de Ville in van Wyk et al op cit at 247. Contra the U.S. case *Roe v Wade* supra.

¹¹⁸³ See also du Plessis & de Ville in van Wyk et al op cit at 247-8, Currie op cit at 307ff, 321.

¹¹⁸⁴ 27 *BVerfGE* 344, 350-355 (1970); *NJW* 555-6 (1970).

¹¹⁸⁵ Cf du Plessis & de Ville in van Wyk et al op cit at 248.

¹¹⁸⁶ 30 *BVerfGE* 1 (1970).

prohibited affected parties from being informed of surveillance under all circumstances was found to violate the principle of proportionality. The court found the amendment permissible but declared the part of the statute that excluded affected parties from being informed void.

5.1.1.1a Relevance to Internet Cafes

Article 1 and 2 of the German Basic Law clearly define the fundamental considerations in the protection of privacy. The protection of human dignity as well as the individual's right to self determination as identified in Articles 1 and 2 are central to and provide a very generous basis for privacy and data protection. Application of this will provide a broad and solid foundation for the protection of privacy and data in Internet cafes.

As seen above, on the basis of Article 2.1, the courts have recognised the right to confidentiality in a variety of cases¹¹⁸⁷ including the confidentiality of personal correspondence.¹¹⁸⁸ Similarly, personal information contained in correspondence or documents processed in Internet cafes should be held as confidential. On the basis of Article 2.1, the German courts have also prohibited general publication of names where such publication might have been unfavourable to the persons involved. In line with this, the publication of personal information over the Internet may also be curtailed or regulated.

¹¹⁸⁷ 65 *BVerfGE* 1, 41-70 (1983); 77 *BVerfGE* 1, 38-63 (1987) (*Neue Heimat*).

¹¹⁸⁸ 35 *BVerfGE* 35 (1973).

The court's recognition in the *Lebach*¹¹⁸⁹ case of the right to determine whether and to what extent others may give a public account of certain aspects of another person's life may also be relevant in determining liability in some cases of Internet publication of personal information.

5.1.1.2 Privacy of Posts and Telecommunications¹¹⁹⁰

Article 10¹¹⁹¹ of the Basic Law states that privacy of correspondence (*Briefgeheimnis*) and privacy of post and telecommunications (*Post- und Fernmeldegeheimnis*) is inviolable.¹¹⁹² Privacy of post has been described as the most comprehensive of all the spheres of privacy protected in Article 10.¹¹⁹³ The content, identity and addresses of the sender and receiver, the content, time and manner of dispatch, and the fact of transmission are all protected under this provision.¹¹⁹⁴ The postal administration has a legal duty to ensure secrecy in all its spheres of activity.¹¹⁹⁵ "Post" in this provision includes letters, parcels, packages, and samples.¹¹⁹⁶

¹¹⁸⁹ 35 *BVerfGE* 202 (1973); *NJW* 1227 (1973).

¹¹⁹⁰ In this section, very few cases were found in the available English texts (including the Internet).

¹¹⁹¹ As amended by Federal Statute of June 24, 1968 (BGBl. I.S. 709).

¹¹⁹² Du Plessis & de Ville in van Wyk et al op cit at 248.

¹¹⁹³ *Ibid.*

¹¹⁹⁴ Cf du Plessis & de Ville in van Wyk et al op cit at 248.

¹¹⁹⁵ See generally du Plessis & de Ville in van Wyk et al op cit at 248.

¹¹⁹⁶ Cf du Plessis & de Ville in van Wyk et al op cit at 248.

Privacy of postal communications however does not afford protection before the correspondence is handed in at the post office and after its delivery.¹¹⁹⁷ This is covered by the part of Article 10 that specifically protects the privacy of correspondence. Privacy of correspondence includes protection against intrusions by public bodies and officials, and generally affords protection in respect of the movement of correspondence outside the sphere of the postal administration.¹¹⁹⁸ The protection guaranteed covers correspondence before it is handed in at the post and after delivery.¹¹⁹⁹ Correspondence includes letters, printed matter, postcards, telegrams, but not, for instance, newspapers.¹²⁰⁰

Privacy of telecommunications affords protection in respect of telegrams, teleprinters, teletex, telefax, long distance calls, and radio-telephones.¹²⁰¹ Telecommunications that take place without the assistance of the postal administration are also protected under this provision.¹²⁰² The protection afforded by this provision extends to both the content of the communication and information regarding the circumstances in which it took place.¹²⁰³ Although the provision does not specifically mention e-mail, it is submitted that given the broad scope of this provision, which covers “telecommunication which takes place

¹¹⁹⁷ See generally du Plessis & de Ville in van Wyk et al op cit at 249.

¹¹⁹⁸ Cf du Plessis & de Ville in van Wyk et al op cit at 249.

¹¹⁹⁹ Ibid.

¹²⁰⁰ Ibid.

¹²⁰¹ Paul Schwartz “German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance” (2003) 54 *Hastings Law Journal* 751.

¹²⁰² See du Plessis & de Ville in van Wyk et al op cit at 249.

¹²⁰³ 85 *BVerfGE* 382, 399 (1992). See also du Plessis & de Ville in van Wyk et al op cit at 249.

without the assistance of the postal administration” (*außerpostalischer Fernmeldeverkehr*)¹²⁰⁴ e-mails are also protected under this provision.

The right is infringed when an official of a public body reads mail, listens in to or records a conversation of a private person or business, makes an order to do so, or enables a third party to do so.¹²⁰⁵ Where, however, one of the participants in a conversation waives his or her right to privacy, and a public body listens in, no infringement has been made.¹²⁰⁶ Article 10.2 specifically sets out the conditions under which the right may be infringed. It has been said that the Article 10 right guarantees the free development of the individual’s personality through the private exchange of information, thoughts and beliefs.¹²⁰⁷ The right to privacy with respect to posts and telecommunications can be claimed by any natural or juristic person,¹²⁰⁸ provided that the person acts as the sender of mail, or takes part in a telephone conversation.¹²⁰⁹

5.1.1.2a Relevance to Internet cafes

Although electronic mail does not ordinarily qualify as “post”, the provisions of Article 10 guaranteeing the privacy of correspondence (*Briefgeheimnis*) and the privacy of

¹²⁰⁴ Cf du Plessis & de Ville in van Wyk et al op cit at 249.

¹²⁰⁵ Cf du Plessis & de Ville in van Wyk et al op cit at 248.

¹²⁰⁶ Ibid.

¹²⁰⁷ Du Plessis & de Ville in van Wyk et al op cit at 248.

¹²⁰⁸ Article 19 (3).

¹²⁰⁹ Ibid.

telecommunications- which includes communications that take place without the assistance of the postal administration-¹²¹⁰ bring e-mail within the purview of this Act. The scope of protection provided for mail and telecommunications also sets a standard and provides a model for similar provisions to be made in Nigeria for the protection of e-mails sent and received in Internet cafes. The protection guaranteed in Article 10 covers the content, identity and addresses of the sender and receiver, the content, time and manner of dispatch, and the fact of transmission in the case of mail.¹²¹¹ For telecommunications, protection under Article 10 covers the content of the communication and information regarding the circumstances in which it took place.¹²¹²

5.1.1.3 The Inviolability of the Home

Article 13.1 provides that the home shall be inviolable. The provisions of this Article protect the right of the occupier.¹²¹³ Thus a person does not have to be the owner of the property to be protected by the provisions of this Article. In effect, tenants, guests, boarders and other persons whose stay on the premises is of a temporary nature may bring an action based on Article 13. “Home” is generously interpreted to include guest-houses, hotel rooms, boats, and places of business as long as the area is not freely

¹²¹⁰ See du Plessis & de Ville in van Wyk et al op cit at 249.

¹²¹¹ Cf above Para 5.1.1.2.

¹²¹² Ibid.

¹²¹³ 75 BVerfGE 318, 326 (1986) “*in Ruhe gelassen zu werden*”. Cf du Plessis & de Ville in van Wyk et al op cit at 250.

accessible to the general public.¹²¹⁴ The protection offered by this Article covers not only permanent fixtures but also moveable structures. It has been said that the rationale is the protection of a spatial sphere where an individual can freely do what he or she pleases.

The right to the inviolability of the home has been interpreted generously to afford protection for individuals, whether they are Germans citizens or foreigners. Domestic, as well as juristic persons are also protected under this article,¹²¹⁵ and protection extends to places that are not strictly private such as places of business. This reinforces the fact that Article 13 protects the right of the occupier.

There are constitutional restrictions on the exercise of the right. Article 13.2 lays down certain conditions¹²¹⁶ under which searches may be carried out. Article 13.3 specifies circumstances¹²¹⁷ under which other intrusions and restrictions may be permitted. In terms of Article 19 of the Basic Law, any of the basic rights may be restricted by legislation in circumstances provided for under the Article.

¹²¹⁴ 32 *BVerfGE* 54 (1971) (*Dry Cleaning* case); 101 *BVerfGE* 361 (1999). Cf du Plessis & de Ville in van Wyk et al op cit at 250.

¹²¹⁵ 32 *BVerfGE* 54, 72 (1971); 42 *BVerfGE* 212, 219 (1976) (*Bauer Company* case). All lawful occupiers of '*Wohnungen*' have a claim to this right. Cf du Plessis & de Ville in van Wyk et al op cit at 250.

¹²¹⁶ These include, where a search is ordered by a judge, or, in circumstances where it would be dangerous to delay taking action, by other organs prescribed by statute. In all cases, the search must be carried out as prescribed by the law. See 75 *BVerfGE* 318, 325 (1986); 59 *BVerfGE* 95, 97 (1982); 51 *BVerfGE* 97, 111 (1978).

¹²¹⁷ Article 13(3) provides: "Intrusions and restrictions may only be made to avert a public danger or a mortal danger to individuals, or, pursuant to a statute, to prevent substantial danger to public safety and order, in particular, to relieve a housing shortage, to combat the danger of epidemics, or to protect juveniles who are exposed to a moral danger."

In line with Article 19, legislation restricting the enjoyment or application of, or legislation authorizing infringements upon, the right to privacy regarding post and telecommunications must mention specifically that the right is to be infringed, must be precise as to the subject matter, purpose and extent of the infringement, and may not encroach on the essence of the right.¹²¹⁸

For instance, if a statute empowers certain officials to intercept correspondence, in the interest of the State, the statute must have a clearly defined subject matter (for instance protection of the State), and must clearly define the purpose for such infringement (for instance, safety and security). The statute permitting interception of correspondence, (which would otherwise be an infringement of a Constitutional right), must also specify the circumstances under which an official may intercept correspondence.¹²¹⁹

In addition, the measure authorizing the infringement has to be in proportion to the aims of the infringement.¹²²⁰ In essence, this provision guards against arbitrary infringement of the rights guaranteed in the Constitution, and aims to ensure that where there is an infringement of any of the rights guaranteed in the Constitution, the degree of

¹²¹⁸ Article 19(2). See generally the *Klass* case: 30 *BverfGE* 1 (1970).

¹²¹⁹ Cf the United States PATRIOT Act of 2001 (Public Law 107-56; 115 Stat. 272), which, for security reasons, permits the interception of communications, in circumstances that might otherwise amount to infringement of the right to privacy. See below Para 4.3.1.13.

¹²²⁰ See 67 *BVerfGE* 157 (1985); NJW 121 (1985), where legislation which allowed the control of letters and telephone calls to countries which had signed the Warsaw treaty was held to be a justified infringement on the right to privacy of posts and telecommunications. Cf du Plessis & de Ville in van Wyk et al op cit at 250.

infringement is limited to the minimum necessary to achieve clearly- stated, valid legal ends.

5.1.1.3a Relevance to Internet Cafes

Although “home” has been interpreted to include places of business and the right afforded in article 13 has been extended to occupiers, it remains doubtful whether Internet café users can benefit from this provision for the following reasons. Firstly, Internet cafes are, by their very nature, often accessible to the public. If, however, it can be shown that the Internet café business is exclusive or not accessible to the public, for instance, where a hotel provides its customers with Internet services, the provisions of Article 13 may be relevant.

Secondly, customers in Internet cafés are neither owners nor occupants, but mere licensees¹²²¹ and as such may not be eligible to bring action under Article 13.

5.1.2 Conclusion on Constitutional Protection of Privacy in Germany

The broad provisions of Article 1.1 and 2.1 may be regarded as a wide blanket affording protection for virtually all forms of invasions of privacy since the right to privacy is essentially the right to determine how, when, where, by whom, and to what extent

¹²²¹ 32 BVerfGE 54 (1971) (*Dry Cleaning* case); 101 BVerfGE 361 (1999). Cf du Plessis & de Ville in van Wyk et al op cit at 250.

personal information about oneself should be used.¹²²² Moreover, in line with Article 1.1, it has been contended¹²²³ that the major interest protected by the law of privacy is human dignity.

The provisions of Article 10 on the privacy of posts and telecommunications are also broad and open regarding the forms of communication covered by the Act thus e-mail communication can be included even though not specifically mentioned. Article 10 is also sufficiently detailed in defining what is protected by the Act and in this regard, its provisions are also generous. Lastly, Article 13 which provides for the inviolability of the home has been construed to protect persons whose stay on premises is temporary. It has also been applied to places of business.

This provision has thus been given a generous interpretation, benefiting categories of persons who would not have benefited given a narrow construction of the provision. It is clear from the cases that both substantive and informational privacy rights are protected. It may thus be concluded that German Constitutional law provides broad based privacy protection with respect to personal space, communication and generally, personal integrity.

¹²²² Cf above Para 1.1.

¹²²³ Cf E J Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 *NYU Law Review* 962, 964; See above Para 1.1.

5.1.2a Relevance to Internet Cafes

In line with the above, it is submitted that as established by the German courts, importance should be attached to the contents of electronic mail as freely written communication.¹²²⁴ In this light, an Internet café user should have a general right to limit disclosure of personal information¹²²⁵ contained in electronic mail, and be compensated for any infringement of this right. The principles enunciated in Articles 1.1 and 2.1 of the German Constitution will thus be useful for the protection of electronic mail in Internet cafes in Nigeria.

Similarly, the provisions of Article 10 on privacy of posts and telecommunications have been regarded as wide enough to accommodate telecommunication that takes place without the assistance of the postal administration.¹²²⁶ In this regard, the protection of content, identity and address of sender, time and manner of dispatch as well as fact of transmission guaranteed by Article 10,¹²²⁷ will apply to electronic mails. Thus, where a person wrongfully discloses information relating to any of the above, there should be liability for such disclosure.

¹²²⁴ Cf 35 BverfGE 311 (1973) (*Prison Correspondence II* case).

¹²²⁵ 1 BVerfGE 65 (1941); Cf du Plessis & de Ville op cit at 246.

¹²²⁶ Cf above Para 5.1.1.2.

¹²²⁷ Ibid.

However, it appears that the provisions of Article 13 will be of little use for the protection of electronic mail in Internet cafes. In this regard, it is submitted that Articles 1.1. and 2.1 together with Article 10 provide a commendable paradigm and constitute ample provisions from German Constitutional law privacy for our purpose and it is unnecessary to attempt to stretch the provisions of Article 13 to cover Internet cafes.

5.1. 3 Constitutional Protection of Data in Germany

In the *Census Act* case,¹²²⁸ the courts, on the basis of Articles 1.1. and 2.1 established the right to informational self-determination. Here, it was affirmed that:

“The individual must be protected from the unlimited collection, storage, use and transmission of personal data as a condition for free personality development under modern conditions of data processing.”¹²²⁹

The court further stated that Articles 1.1 and 2.1. guarantee the right of the individual to determine for himself, or herself whether personal data relating to them may be used.¹²³⁰ It has also been observed that the right to informational self-determination would be violated where automatic data processing and the sharing of statistical data with local and

¹²²⁸ 65 *BVerfGE* 1 (1983).

¹²²⁹ 65 *BVerfGE* 1 (1983). Cf Kommers op cit at 325.

¹²³⁰ *Ibid.*

regional authorities could result in the reconstruction or release of the personality profiles of particular individuals.¹²³¹

The courts have also held that to require a person to register and record all aspects of his or her personality, even though it is carried out anonymously in the form of a statistical survey, would be a violation of the right to self-determination contained in Article 2.1 of the German Basic Law.¹²³²

The courts have, in upholding the right to informational self-determination, also limited disclosure of medical records¹²³³ and divorce files.¹²³⁴

5.1.3a Relevance to Internet Cafes

As observed above,¹²³⁵ the right to self determination is central to data (and privacy) protection and many forms of data (and privacy) invasions would be outlawed on this basis. Based on Articles 1.1. and 2.1, Internet café users would have the right to limit and/or regulate access to, disclosure of, publication and other use of personal information in Internet cafes.

¹²³¹ 65 BVerfGE 1, 41-70 (1983). Cf du Plessis & de Ville in van Wyk op cit at 247.

¹²³² 27 BVerfGE 1,6 (1969).

¹²³³ 32 BVerfGE 373, 378-86 (1972) (*Medical Confidentiality case*).

¹²³⁴ 27 BVerfGE 344, 350-355 (1970).

¹²³⁵ Para 5.1.1.1a.

5.1.4 Conclusion on Constitutional Protection of Data in Germany

The right of the individual to determine for himself, or herself whether [and how] personal data relating to them may be used, and the correlating need for limitation of the collection, use and storage of personal information, as enunciated by the German courts,¹²³⁶ may be regarded as fundamental elements of data protection law. These are the core considerations in the German constitutional law protecting data.

In this regard, the German courts have recognised the need to regulate and limit various aspects of data processing that result in violations of privacy including data collection,¹²³⁷ storage,¹²³⁸ sharing,¹²³⁹ and disclosure.¹²⁴⁰ In affirming the right to informational self determination, the courts have also upheld the right of the individual to decide who may have information about them;¹²⁴¹ to know who is in possession of personal information regarding them. In conclusion, it may be said that German constitutional law provides a firm foundation on which a strong data protection law can be built.

5.1.4a Relevance to Internet Cafes

¹²³⁶ 65 *BverfGE* 1 (1983).

¹²³⁷ *Ibid.* See also 27 *BVerfGE* 1, 6 (1969).

¹²³⁸ 65 *BverfGE* 1 (1983).

¹²³⁹ 65 *BVerfGE* 1, 41-70 (1983).

¹²⁴⁰ 32 *BVerfGE* 373, 378-86 (1972); 27 *BVerfGE* 344, 350-355 (1970).

¹²⁴¹ 65 *BverfGE* 1 (1983).

The data protection rights recognised in the German Constitution will be relevant for the protection of information processed in Internet cafes. General application of the German constitutional right to informational self-determination will confer on an Internet café user extensive protection against unauthorised use of personal information processed in Internet cafes. Such protection will include the right to the limitation of collection, storage, use and disclosure of such information. In conclusion, German constitutional law offers valuable principles for the protection of privacy in Internet cafes in Nigeria.

5. 2 Civil Law Protection of Privacy and Data in Germany

5. 2. 1 Civil Law Protection of Privacy

The German Civil Code¹²⁴² does not recognise a general right to privacy.¹²⁴³ However, many invasions of privacy have been recognised under the principles of personality rights, based on the *actio injuriarum*.¹²⁴⁴ In effect, although there was no civil action for the protection of privacy rights, the courts recognised individual interests regarding privacy and the law evolved as in the case of the United Kingdom and the United States.¹²⁴⁵

¹²⁴² *Bürgerliches Gesetz Buch* of 1896, as amended by Act of 25 June 1998.

¹²⁴³ See McQuoid-Mason *op cit* at 57ff.

¹²⁴⁴ *Ibid.*

¹²⁴⁵ *Ibid.*

Article 823 and Article 826 of the German Civil Code (BGB)¹²⁴⁶ are the two major provisions that deal with protection of privacy. Article 823 (1) provides that:

“One who intentionally or negligently, wrongfully injures the life, body, health, freedom, property or any other right of another is obligated to compensate him for damage arising therefrom.”¹²⁴⁷

Article 823, protects against intentional or negligent injury to the life, body, health, liberty, property rights or “any other right” of another person. It has been contended that the words “any other right” should be construed strictly to exclude the right to privacy, not expressly mentioned in the first paragraph of the Article.¹²⁴⁸ Relying on the *eiusdem generis* rule,¹²⁴⁹ it has been argued that the personality rights intended to be recognised in Article 823 are specifically listed and the words, “other rights” refer to proprietary rights, as suggested by the inclusion of “property” in the provision. On this basis, the interest in protecting the integrity of the personal sphere, or preserving honour and reputation, are excluded from the scope of protection of the first paragraph of Article 823.¹²⁵⁰

¹²⁴⁶ *Bürgerliches Gesetz Buch* of 1896 as subsequently amended.

¹²⁴⁷ Translation by H D Krause “The Right to Privacy in Germany- Pointers for American Legislation?” (1965) Vol *Duke Law Journal* 481 at 518. Cf McQuoid-Mason op cit at 59. See also Markesinis op cit at 10.

¹²⁴⁸ See H Stoll “The General Right to Personality in German Law: An Outline of its Development and Present Significance” in Markesinis *Protecting Privacy* op cit at 29.

¹²⁴⁹ The rule states in essence that the express mention of a thing or a specific category excludes others that are not in the same category.

¹²⁵⁰ Cf 69 RGZ 404f (1908) where the courts refused the plaintiff’s action to prevent the publication of letters on the basis of personality rights, but subsequently allowed the action on the basis of German copyright law. See also Stoll in Markesinis *Protecting Privacy* op cit at 29, 30.

However, in 1957, the (*Bundesgerichtshof*) held that the right to privacy could be protected under the Article although its scope in each case would be limited by balancing the values and interests involved.¹²⁵¹ In effect, negligent and intentional invasions of personality rights would be actionable under Article 823. This decision has received approval and has been followed in a number of other cases.

In the *Herrenreiter* case,¹²⁵² the photograph of a famous horse rider was used without his consent to advertise a patent medicine to improve sexual potency. Article 823 was successfully invoked to protect the plaintiff's personality rights. Similarly where a professor of law was depicted without his authority as an important scientist expressing an opinion in an advertisement for a tonic, he was awarded damages for the unauthorised attack on his personality.¹²⁵³

The second paragraph of Article 823 deals with tortious liability for infringement of statutory rules. It "imposes an obligation to make amends on anyone who violates a statutory provision intended for the protection of others."¹²⁵⁴ Although it has been suggested that the protection of personality rights provided here is subject to the

¹²⁵¹ Krause "The Right to Privacy in Germany- Pointers for American Legislation?" (1965) *Duke Law Journal* 481 at 522f.

¹²⁵² 26 BGHZ 349 (1958).

¹²⁵³ 35 BGHZ 363 (1961), NJW 2059 (1961).

¹²⁵⁴ See Markesinis *The German Law of Torts* at 10, 653.

existence of a criminal offence relating to personality,¹²⁵⁵ it is arguable that violations of Articles 1 and 2 of the Basic Law would also invoke liability under this law.

In a case¹²⁵⁶ where the plaintiff's sperm, which had been frozen prior to an operation that resulted in his impotency, was negligently destroyed, the court granted the plaintiff relief for immaterial loss by analogous application of the principle requiring a wrongdoer to indemnify his/her victim in respect of immaterial loss for tortuous injury to the body. The court justified the analogy by "the personality right of the person entitled".¹²⁵⁷ In this case, the court regarded injury to the plaintiff's sperm as injury to his body and fitted this under Article 823, which requires anyone who "recklessly or negligently injures the life, body, health, freedom, property, or other right of another contrary to law"¹²⁵⁸ to compensate the plaintiff.¹²⁵⁹

Personality interests not protected by the first paragraph of Article 823 may be protected under the second paragraph or under Article 826, which provides that "one who intentionally damages another in a manner violating good morals is obliged to compensate him for such damages."¹²⁶⁰ This provision is a general clause imputing

¹²⁵⁵ See Stoll in Markesinis *Protecting Privacy* op cit at 30.

¹²⁵⁶ Cf BGH 9, 11 (1993), 52 BGHZ 124 (1993).

¹²⁵⁷ Ibid at 57.

¹²⁵⁸ See translation in Markesinis *The German law of Torts* op cit at 10.

¹²⁵⁹ This decision has been criticised on the grounds that the courts should have based their decision on the protection of personal dignity rather than the right to bodily integrity. Christian von Bar *The Common European Law of Torts* Volume 1 (1998) at 609.

liability for the intentional infliction of damage to another in a manner contrary to good morals.

It has also been contended that Article 826 of the German Civil Code provides for the recognition of different personality rights not specifically mentioned in the Code.¹²⁶¹

Thus the Article could be construed to cover intentional invasions of privacy violating “good morals”,¹²⁶² for instance, where a defendant made a privileged disclosure to his clients concerning the plaintiff’s criminal conviction and such privilege was exceeded.¹²⁶³

It appears however that the role of Articles 1 and 2 of the German basic Law in the development of a right to privacy cannot be neglected. In this regard, it has been suggested¹²⁶⁴ that there was a general pragmatic development of personality right protection on the basis of Article 826 of the Civil Code and, of Articles 1 and 2 of the Federal Constitution.¹²⁶⁵

¹²⁶⁰ Translation in Justice Report *Privacy and the Law* (1970) at 21f Para 97; See also Markesinis *The German Law of Torts* op cit at 11.

¹²⁶¹ J Kohler *Personlichkeitsrecht* 1, 587; W. A Joubert “ Die Persoonlikheidreg : ’ n Belangwekkende Ontwikkeling in die Jongste Regspraak in Duitsland” (1960) 23 *THRHR* 30; See McQuoid-Mason op cit at 58.

¹²⁶² Krause (1965) *Duke Law Journal* 481 at 487.

¹²⁶³ 115 RGZ 416 (1927); Krause (1965) *Duke Law Journal* 481 at 487f.

¹²⁶⁴ Justice *Privacy* op cit 21 Para 97.

¹²⁶⁵ *Grundgesetz* (1949) as subsequently amended. Cf E J Cohn *Manual of German Law* 2 ed (1968) who states that ‘the “right to privacy” is derived by a somewhat strained interpretation from Arts 1 and 2 from the Basic Law.’

In the landmark *Schacht* case,¹²⁶⁶ the plaintiff, an attorney, wrote to a newspaper on behalf of his client, demanding that the paper correct certain statements made about his client. The paper however published the attorney's letter so that it appeared that he had written in his personal capacity. The attorney succeeded in obtaining an order to compel the paper to correct the false impression by publishing a statement that he had not written in his personal capacity. The BGH held that on the basis of Articles 1 and 2 of the Basic Law, which guaranteed the inviolability of human dignity as well as the free development of personality as fundamental rights, the courts could grant protection for personality interests.¹²⁶⁷

This principle has been followed in subsequent decisions by the courts.¹²⁶⁸ In the *Princess Caroline of Monaco* case,¹²⁶⁹ where the defendants published incorrect reports as well as a false "exclusive" interview with the plaintiff, the plaintiff was granted damages for repeated attacks on her personality.

5.2.1a Relevance to Internet Cafes

Article 823 will be relevant for the protection of privacy in Internet cafes where there is injury to the life, body, health or liberty in invading the plaintiff's privacy. For instance,

¹²⁶⁶ 13 BGHZ 334 (1954).

¹²⁶⁷ See Krause (1965) *Duke Law Journal* 481 at 488f.

¹²⁶⁸ *Wagner's Case* 15 BGHZ 249 (1954); *Paul Dahlke Case* 20 BGHZ 345 (1956).

¹²⁶⁹ BGH 15, 11 (1994), 128 BGHZ 1 (1994); NJW 861 (1995).

where the plaintiff is beaten up and injured in order to obtain personal information processed by him/her in an Internet cafe. On the basis of *Herrenreiter*¹²⁷⁰ there will also be liability for invasion of privacy where personal information is unlawfully published or otherwise used in a manner that violates the plaintiff's personality rights.

There will be liability under the second part of Article 823 only where the act complained of constitutes a violation of another law. For instance, where a computer in an Internet café is stolen in order to access and publish personal information contained in the computer's hard drive, the act of stealing constitutes a contravention of the Nigerian Criminal Code for which there will be liability under the second part of Article 823.

Further to this, Article 826 of the Civil Code which has been construed to cover intentional invasions of privacy violating good morals may be interpreted to prohibit unauthorised disclosure, publication or other use by Internet café personnel of personal information relating to customers.¹²⁷¹ The basis for this is the argument, as submitted above,¹²⁷² that Internet café personnel ought to be under a moral duty to maintain confidentiality with respect to information processed in their Internet cafes.

From the above, it may be said that, although the Civil Law principles from which privacy rights can be drawn are not cohesive, German Civil Law contains relevant provisions that may be adapted for the protection of privacy in Nigerian Internet cafes.

¹²⁷⁰ *Supra*.

¹²⁷¹ 115 RGZ 416 (1927); Krause (1965) *Duke Law Journal* 481 at 487ff.

5.2.2 Civil Law Protection of Data in Germany

There is no specific Civil Law provision on, or protection against, the misuse of information stored in a data bank in Germany. However, German Civil Law affords general protection for data where information is unlawfully obtained or where publication or disclosure of information constitutes an invasion of privacy or personality rights as recognised under the general principles of Civil Law. In this regard, if the injured party can show that the information has been unlawfully obtained or that the information affects his or her honour or business reputation, or that it concerns his or her sex life,¹²⁷³ they may be protected under Civil Law principles.

The provisions of Article 824 may also give rise to a claim where a person publishes wrong facts that endanger the credit of the plaintiff, in circumstances where the person who published the information knows, or ought to know that the information is false.¹²⁷⁴

Article 824 provides that:

“A person who maintains or publishes, contrary to the truth, a statement calculated to endanger the credit of another, or to injure his earnings or prospects in any other manner, must compensate the other for any damage

¹²⁷² Para 3.2.2.1.1.1a.

¹²⁷³ See generally J Neethling *Neethling's Law of Personality* (2005) at 108-112; McQuoid- Mason op cit at 64.

¹²⁷⁴ Cf Markesinis *The German Law of Torts* op cit at 56.

arising therefrom, even if he does not know of its untruth, provided he ought to know.”¹²⁷⁵

This provision may offer protection against negligent or intentional publication of untrue and potentially-damaging information by data agencies and their officials. It will also be relevant in cases where information that places another in a false light is published. Article 12 of the BGB also protects the human name.¹²⁷⁶

5.2.2a Relevance to Internet Cafes

Article 824 of the German Civil Code will be particularly relevant for the prevention of, or for the compensation of plaintiffs in cases of, negligent or intentional disclosure or publication of information processed in Internet cafes where such information is untrue and capable of damaging the plaintiff's credit. The data protection afforded by German Civil law will be also be relevant in Internet cafes where information is unlawfully obtained, disclosed, published or otherwise used in a manner that adversely affects the plaintiff's honour, business reputation, sex life or any other personality right recognised under Articles 823 and 826 of the Civil Code.

5.3 Statutory Protection of Privacy and Data in Germany

¹²⁷⁵ Translation in Markesinis *The German Law of Torts* op cit at 11.

¹²⁷⁶ Cf Markesinis *The German Law of Torts* op cit at 56.

5.3.1 Statutory Protection of Privacy¹²⁷⁷

Certain laws contain isolated provisions on the protection of privacy. The Law of Artistic Creations¹²⁷⁸ contains provisions on the right to one's likeness and prohibits the unauthorised publication of one's likeness.¹²⁷⁹ In the *Mephisto* case,¹²⁸⁰ the plaintiff sought to restrain the publication of a book that clearly described his deceased father even though some of the details contained in the book were fictitious. The court granted posthumous protection of the personality on the basis of Article 22 of the Law of Artistic Creations.

The German Copyright Act¹²⁸¹ also offers limited protection for the infringement of "personal intellectual creations."¹²⁸² In an action by Friederich Nietzsche's relatives to prevent the threatened posthumous publication of certain letters, the action was allowed on the basis of copyright.¹²⁸³ To qualify for protection under the Act however, such

¹²⁷⁷ Most of the German statutory provisions that the researcher found were in the German language with no translations available. Since the researcher does not speak or understand the German language, this placed a limitation on the number of statutes available for examination in this paragraph.

¹²⁷⁸ *Kunsturhebergesetz* (1907).

¹²⁷⁹ Articles 22 ff.

¹²⁸⁰ 30 *BverfGE* 173 (1971), BGH 20.3 (1968).

¹²⁸¹ *Urheberrechtsgesetz* (1965) Article 2(2).

¹²⁸² Articles 2 (2). Cf C Reed *InternetLaw: Text and Materials* (2004) at 7,8.

¹²⁸³ 69 RGZ 404f (1908).

creations must display a degree of creativity higher than the average level in the field in question.¹²⁸⁴

5.3.1a Relevance to Internet Cafes

The *Mephisto* case¹²⁸⁵ underlines an important factor in the examination of the different statutes that are not Data Protection Acts, examined in this work. Even where there is an exhaustive Data Protection Act in place, certain subject-specific statutes may provide more effective protection in certain instances. Subject-specific statutes thus have their significance and cannot be disregarded in the protection of privacy and data.¹²⁸⁶

The *Mephisto* case¹²⁸⁷ provides an apposite illustration of generous construction of statute law, in a case where protection might not ordinarily be available under ordinary data protection legislation; case in point: for the protection of a deceased person. The court's unrestrictive approach in the *Mephisto* case is noteworthy and it is suggested that Nigerian courts adopt a similar generous approach in the construction of any law protecting privacy and data in Internet cafes in Nigeria.

5.3.2 Statutory Protection of Data

¹²⁸⁴ *Inkasso-Programm* BGH decision of 9 May 1985, 1986 IIC 681; *Betriebssystem*, BGH decision of 4 October 1990, 1991 IIC 723. Cf Reed op cit at 8.

¹²⁸⁵ Supra.

¹²⁸⁶ Cf above Para 3.2.3.1.2.4a.

¹²⁸⁷ Supra.

The Federal Data Protection Law¹²⁸⁸ governs data protection in Germany. The law covers the collection, processing and use of personal data collected by public federal and state authorities, (where there is no state regulation), and of non- public offices as long as they process and use the data for commercial or professional aims.¹²⁸⁹ The general purpose of the Act is to protect the individual against violations of his ‘personal rights’ (*personlichkeitsrecht*) that may arise from the handling of person-related data.¹²⁹⁰

The Act covers automated and non-automated files.¹²⁹¹ “Personal data” is defined in the Act as “any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).”¹²⁹² The Act requires that personal data be collected from the data subject¹²⁹³ and prescribes conditions for collecting such data without the data subject’s participation.¹²⁹⁴ Data protection in Germany is demarcated on the basis of public law and private law,¹²⁹⁵ thus the Act contains

¹²⁸⁸ *Bundesdatenschutzgesetz*; Federal Data Protection Act of 27 January 1977 BGBl. I.S. 2325 last amended 23 May 2001. Cf 20 December 1990 Federal Law Gazette 1 1990 at 2954. Cf http://www.bfd.bund.de/information/bdsg_eng.pdf or http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm for English version of the Act.

¹²⁸⁹ Section 1 (2). Cf The Green Paper on Electronic Commerce for South Africa op cit at Para 8.65.

¹²⁹⁰ Part I Section 1(1).

¹²⁹¹ Part I Section 3(2).

¹²⁹² Part I Section 3(1).

¹²⁹³ Section 4(2).

¹²⁹⁴ Section 4(2) (1& 2).

¹²⁹⁵ Cf Germany: The Federal Data Protection Commissioner at http://www.bfd.bund.de/information/datprotec_en.html. Accessed December 2004.

provisions on data processing by public bodies,¹²⁹⁶ and data processing by private bodies.¹²⁹⁷

Rights of the data subject under the Act include the right of access,¹²⁹⁸ as well as the right to correction, erasure and blocking of data.¹²⁹⁹ These are regarded as inalienable rights of the data subject and they may not be excluded or restricted by a legal transaction.¹³⁰⁰ Under the Act, the right of access includes the provision of information to the data subject about stored data concerning him or her,¹³⁰¹ and notification¹³⁰² (of the data subject), where data is collected without his/ her knowledge. The Act provides for clear specification of the purpose(s) for which data is to be used,¹³⁰³ and requires collection, processing and use of data to be in accordance with the specified purpose(s),¹³⁰⁴ or, in accordance with the exemptions specified in the Act.¹³⁰⁵ The data subject also has a right of objection to the collection, use or processing of data.¹³⁰⁶

¹²⁹⁶ Part II Chapter II.

¹²⁹⁷ Part III Chapter II.

¹²⁹⁸ Sections 19, 34.

¹²⁹⁹ Sections 20, 35.

¹³⁰⁰ Section 6.

¹³⁰¹ Sections 19, 34.

¹³⁰² Section 19(a), Section 33.

¹³⁰³ Section 28(1).

¹³⁰⁴ Sections 28, 39, 40.

¹³⁰⁵ Section 28(2), (3) & (4).

¹³⁰⁶ Section 20, Section 35.

The Act contains other provisions on access to data, confidentiality and enforcement of the Act to increase its effectiveness. In this regard, the Act makes provision for supervisory authorities to keep a register of automated data banks containing personal information, which the public may consult, to facilitate access to data banks.¹³⁰⁷ The Act also makes provision for a Federal Data Protection Commissioner to whom appeals may be made by any aggrieved person in respect of an alleged infringement of his or her data protection rights.¹³⁰⁸

Further to this, the Act prohibits persons employed in data processing from collecting, processing or using personal data without authorization and requires that such employees give an undertaking to maintain confidentiality.¹³⁰⁹ This undertaking of confidentiality remains valid after termination of activity or work.¹³¹⁰

In addition, the Act provides for compensation by public¹³¹¹ and private¹³¹² data controllers in respect of inadmissible or incorrect collection, processing or use of data that results in harm to the data subject. Furthermore, the Act provides for criminal¹³¹³ as

¹³⁰⁷ Section 38(2).

¹³⁰⁸ Section 21.

¹³⁰⁹ Section 5.

¹³¹⁰ Ibid.

¹³¹¹ Section 7.

¹³¹² Section 8.

¹³¹³ Section 43.

well as administrative ¹³¹⁴ offences in respect of certain acts of non-compliance with the Act, for which there will be liability.

The Federal Data Act was updated in 2001 to make it consistent with the European Union Data Protection Directive.¹³¹⁵ The Act now includes regulations on transmitting personal data abroad¹³¹⁶, depersonalisation,¹³¹⁷ pseudonymisation,¹³¹⁸ video surveillance¹³¹⁹ and mobile personal data processing systems.¹³²⁰ These recent regulations provide for the collecting, processing and use of as little personal data as possible in the organisation and choice of data-processing systems.¹³²¹ In addition, the Act grants data subjects greater rights of objection.¹³²²

¹³¹⁴ Section 44.

¹³¹⁵ Directive 95/46/EC 1995.

¹³¹⁶ Section 4(b).

¹³¹⁷ Section 3(6) defined in the Act as “the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.” (Also referred to as “anonymisation” in the Act; Section 3(a))

¹³¹⁸ Section 3(6a). Pseudonymisation is defined in the Act as “the replacement of the name and other identifying attributes with a code with a view to making it impossible or significantly more difficult to identify the data subject.”

¹³¹⁹ Section 6(b).

¹³²⁰ Section 6(c). Cf generally, The Green Paper on Electronic Commerce for South Africa op cit at Para 8.6.7.

¹³²¹ Section 3(a).

¹³²² Ibid.

Furthermore, the Act provides for the appointment of a data protection official by public and private bodies that collect, process or use personal data.¹³²³ The appointed official will, in addition to complying with the general provisions of the Federal Data Act,¹³²⁴ be bound to maintain secrecy on the identity of data subjects and on circumstances permitting conclusions to be drawn about a data subject.¹³²⁵

A key distinctive feature of German data protection law, is its dual system of administration whereby the data laws operate both at the federal level and at the state level. There are commissions in each of the *Länder*(s) that enforce the *Länder* data protection Acts¹³²⁶ while the Federal Data Protection Commission (*Bundesbeauftragter für den Datenschutz*) is responsible for supervision of the Federal Data Protection Act.¹³²⁷

The availability of administrative supervision at the state level will enhance effective monitoring to ensure compliance with its provisions. Effective monitoring and thorough administration of the laws is also ensured through the creation of separate governmental bodies to administer them.

¹³²³ Section 4(f).

¹³²⁴ Section 4(g)(1).

¹³²⁵ Section 4(f)(4).

¹³²⁶ E.g Berlin, Bremen Hamburg, Lower Saxony Cf The Federal Data Protection Commissioner at Accessed December 2004. All *länders* have their own specific data protection registries that cover the public sector of the *Lander* administration.

¹³²⁷ Section 24 on monitoring of compliance http://www.bfd.bund.de/information/datprotec_en.html. Cf D Banisar & S Davies "Privacy and Human Rights: An International Survey of Privacy Laws and Practice" (1999) <http://www.gilc.org/privacy/survey/intro.html> Accessed September 2000.

Reference must also be made to Section 6 of the German Act which provides for inalienable rights of data subjects.¹³²⁸ In effect, any provisions that infringe on these rights in any legal transaction will be void, similarly any transactions constituting a violation of any of these rights will be annulled. This provision underlines the importance attached to data protection by the Germans, firmly secures these rights and emphasises the recognition of data protection rights as fundamental human rights.

5.3.2a Relevance to Internet Cafes

Most of the provisions of the German Data Act are, in content and effect, comparable to those of the United Kingdom Data Act,¹³²⁹ and as such, the provisions highlighted in the United Kingdom Act as essential components of any data protection law and therefore significant for the protection of information processed in Internet cafes,¹³³⁰ will be equally relevant in the German Act. These will include provisions regarding the rights of data subjects, duties of data controllers, and other features in the Act which are subsumed in the data protection principles.¹³³¹ The discussion of the relevance of the data protection principles will be done in detail below.¹³³²

¹³²⁸ Viz: the right to information, correction, erasure or blocking; Sections 19, 34 and Sections 20, 35.

¹³²⁹ Both Data Acts were revised to conform to the EU standard. Cf above Paras 3.2.3.2 and 5.3.2.

¹³³⁰ Cf above Para 3.2.3.2.2.5 ff.

¹³³¹ Cf above Para 3.2.3.2.2.5

¹³³² Chapter 9.

The major point of departure between the German and United Kingdom Data Acts will be in the German law dual administrative system, which, as will be seen,¹³³³ may also be relevant for data protection and the protection of information processed in Internet cafes in Nigeria.

5.3.3 Other Statutes

There are other statutes under which information and data are protected. For instance, the Telecommunications Carriers Data Protection Ordinance of 1996¹³³⁴ protects the privacy of telecommunications. The Information and Communication Services (Multimedia) Act of 1997¹³³⁵ provides protection for information used in computer networks. Under the Federal Law to regulate the Conditions for Information and Communication Services 1997, intermediaries, such as Internet Service Providers (ISP's), are responsible for their own content which they make available for use.¹³³⁶ By virtue of the same law, where Internet Service Providers host unlawful content on their servers, they will be liable for such¹³³⁷ if:

- (a) they know that the content is unlawful,

¹³³³ Ibid.

¹³³⁴ Telecommunications Carriers Data Protection Ordinance (TDSV) 12 July 1996.

¹³³⁵ *IuKDG* 1997; Also cited as Federal Act Establishing the General Conditions for Information and Communication Services, 13 June 1997; also known as the Multimedia Law 1997.

¹³³⁶ Article 5 (1) Transl. Christopher Kuner, www.kuner.com. Cf Reed op cit at 114.

¹³³⁷ Article 5.

- (a) it is technically possible for the intermediary to block access to the use of the information, and
- (b) it is reasonable to expect such blocking to be effected.¹³³⁸

In essence, where a person's privacy is invaded by the publication of unlawful information on the Internet, if the source of the information is the Internet Service Provider, they will be liable for its publication. If, however, the information does not originate from the Service Provider, but the Service Provider knows the nature of the information and fails to take reasonable steps to block its access or use, the Internet Service Provider will be liable for the publication of the information.

This provision is in line with the European Community Directive on Electronic Commerce 2000.¹³³⁹ Germany is also a member of the Council of Europe and The European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data is also applicable to Germany.¹³⁴⁰

5.3.3a Relevance to Internet Cafes

The Federal Law to regulate the Conditions for Information and Communication Services 1997 contains provisions that will be relevant in making Internet Service Providers responsible for invasions of privacy arising from the publication of, or for failure to

¹³³⁸ Article 5(2). Cf Reed op cit at 114.

¹³³⁹ Directive 2000/31/EC OJ L 178 p.1, 17 July 2000.

remove, information posted on their servers. Internet Service Providers are capable of publishing, and they possess the technology to block access to material. Internet Service Providers will thus be responsible for their publication of information constituting an invasion of privacy and for the failure or neglect to remove such material.

This provision provides practical and effectual privacy protection since the removal of information constituting privacy invasion will be more beneficial to a plaintiff than the award of damages after the fact. The inclusion of similar provisions in any privacy and data law for Internet cafes will enhance effective privacy protection for information processed in Internet cafes.

5.4. Conclusion on German Law Protection of Privacy and Data

5.4.1 Conclusion on German Law Protection of Privacy

The protection offered by the privacy laws of Germany is rooted to a great extent in the Constitution. Although the constitutional provisions guaranteeing the right to privacy also contain restrictions, these restrictions are useful to serve as checks and balances. On the one hand, they provide guidelines and parameters within which the judiciary and the administrative bodies regulating compliance with the provisions of the law relating to privacy can work. On the other hand, they delimit the scope of the enjoyment of the right

¹³⁴⁰ EU Directive 95/46/EC 1995; See above Para 3.2.3.2.1.

to privacy. This is necessary for every right,¹³⁴¹ particularly so, the right to privacy, considering the “elusive and amorphous”¹³⁴² nature of the right.

The preceding examination of the constitutional provisions guaranteeing the right to self-determination,¹³⁴³ privacy of posts and telecommunications¹³⁴⁴ and privacy of the home,¹³⁴⁵ show that they have been interpreted broadly and generously by the courts. To this extent, and to the extent that the restrictions in the constitutional guarantee of the right to privacy have been interpreted constructively, it may be argued that German Constitutional law offers a better model for privacy protection than the United States Constitution.

The German Civil Code also provides for the right to privacy and the courts have construed this broadly to protect personality rights. However, the absence “of a unitary conception and fragmentary protection of personality rights”¹³⁴⁶ by the Civil Code have been described as unsatisfactory,¹³⁴⁷ and other shortcomings of the Civil Code¹³⁴⁸ have

¹³⁴¹ Cf above Para 1.1.

¹³⁴² Ackermann J in *Bernstein v Bester* supra at 791 Para 65.

¹³⁴³ Article 1.1, Article 2.1; Cf above Para 5.1.1.1.

¹³⁴⁴ Article 10; Cf above Para 5.1.1.2.

¹³⁴⁵ Article 13; Cf above Para 5.1.1.3.

¹³⁴⁶ Stoll in Markesinis *Protecting Privacy* op cit at 31.

¹³⁴⁷ Ibid.

¹³⁴⁸ For instance, although the Civil Code excludes damages for immaterial loss not expressly provided for by law, (Articles 253, 847), in the *Herrenreiter* case supra, the court held that there had been a serious infringement of the plaintiff's general right to personality and he was awarded damages for immaterial loss on the basis of Articles 1 and 2 of the Basic Law.

received criticism.¹³⁴⁹ In particular, the decisions of the courts extending the scope of the Civil Code to allow the protection of a general right of personality have been criticised.¹³⁵⁰ In spite of these criticisms, the Civil Code is being increasingly used to protect personality rights.¹³⁵¹

It is submitted that the use of the Civil Code to protect personality rights is a positive development for the law of privacy. In this regard, it is submitted that, although the German Civil Code development of the right to privacy has been on a case-by-case basis, this development has not been altogether arbitrary. It may be said in its favour that there has been method in the Civil Code development of the right to privacy, based on the foundation of the existing Civil Code,¹³⁵² and, evidenced by the fact that the essential elements necessary to be proved in all cases are consistent.¹³⁵³ As such, it is submitted that the basis and scope of protection afforded by the German Civil Law right to privacy is reasonably clear and sufficiently defined to provide a unifying common factor.

¹³⁴⁹ Stoll in Markesinis *Protecting Privacy* op cit at 31.

¹³⁵⁰ See generally Stoll in Markesinis *Protecting Privacy* op cit at 31.

¹³⁵¹ 34 BverfGE 269 (1973) where the Constitutional Court held that the use of civil law to extend and give effect to these constitutional provisions did not constitute a violation of the Constitution. Cf Markesinis *The German Law of Torts* op cit at 57. See also McQuoid-Mason *The Law of Privacy in South Africa* op cit at 60.

¹³⁵² Articles 823 and 826 of the Civil Code. Cf above Para 5.2.1.

¹³⁵³ There are general standard requirements laid down for an action to succeed under any of these heads. Article 823 gives relief mainly for invasions of privacy in cases of negligent and intentional invasions of personality rights (see 35 BGHZ 363 (1961); *Herrenreiter* 26 BGHZ 349 (1958)), while Article 826 deals with intentional invasions of privacy violating good morals (see *Schacht* 13 BGHZ 334 (1954); *Princess Caroline of Monaco* BGH 15, 11 (1994)). Cf above Para 5.2.1.

Furthermore, it is submitted that the “fluid” nature of the Civil Code development of the right to privacy allows for legal development that is at par with technological advancements and is necessary to address the issue of present day threats to privacy. The courts have merely utilised the existing provisions of the law to guarantee a broad base of protection for citizens in circumstances not specifically pre-empted or provided for by the law. In so doing, they have construed the letter of the law to fulfill the spirit of the law, which, it is submitted, is to be commended.

It is suggested that if, in the future, the development of the right to privacy based on the Civil Code is to be regulated, such regulation should strive to maintain a balance between the flexibility to accommodate societal changes so as to ensure effectiveness, and the need for certainty in the law, to avoidance arbitrariness.

Finally, other positive aspects of German law privacy protection include the fact that Civil law protection of privacy is not confined to German citizens, but foreigners are clearly included, and that domestic juristic persons may also enjoy Basic Rights concerning privacy where the nature of the rights permits them to do so.¹³⁵⁴ It may be concluded from the preceding that in spite of its shortfalls, German law privacy protection is built on a solid foundation. It is also sufficiently flexible to provide protection for a variety of acts amounting to privacy invasion and to allow the development of the privacy laws to reflect societal changes and thus remain relevant.

¹³⁵⁴ Article 19(3).

5.4.1a Relevance to Internet Cafes

The relevance of the different aspects of German law to Internet cafes has been shown in the preceding paragraphs. It will however be emphasised in conclusion that the creativeness of the German Civil courts in construing the available law to allow for protection of privacy needs is highly commendable and particularly instructive for the Nigerian courts. In the absence of previous invasion of privacy cases in Nigeria, the courts must be proactive in developing privacy rights and sensitive in adapting them to fit the society in terms of contemporary needs for its current stage of development. In this regard, Internet cafes will be a major consideration in Nigeria. In sum, it will be reiterated that German law offers valuable principles for the development of a privacy and data law for use in Internet cafes in Nigeria.

5.4.2 Conclusion on German Law Protection of Data

German data protection laws are consistent with European Union Data Protection Directive¹³⁵⁵ and as such, they conform to a high standard, set and recognised by an International body.¹³⁵⁶ In this regard, several significant features of the German Data Act have been highlighted.¹³⁵⁷ Although the Federal Data Act is comprehensive, other Acts also exist under which limited data protection can be found in respect of specific subjects thus reinforcing the available data protection.

¹³⁵⁵ EU Directive 95/46/EC (1995); Cf above Para 3.2.3.2.1.

¹³⁵⁶ Cf above Paras 3.2.3.2.1 ff.

Very significantly, the administrative model for the German Data Act has been designed to reflect the nature of the country, thus enhancing the potential of the Act for success. In conclusion, it is submitted that German data laws provide an outstanding standard of protection for data subjects.

5.4.2a Relevance to Internet Cafes

As observed above, the German Federal Data Act provides an excellent standard of data protection and it is submitted that the adoption/adaptation of the principles espoused in the German Act will be highly profitable for the protection of data in Internet Cafes in Nigeria.

¹³⁵⁷ Cf above Para 3.2.3.2.1.2 and Para 3.2.3.2.2.5.

CHAPTER SIX

COMMON LAW PROTECTION OF PRIVACY AND DATA IN SOUTH AFRICA AND NIGERIA

6.1 Common Law Protection of Privacy and Data in South Africa

6.1.1 Common Law¹³⁵⁸ Protection of Privacy

Although a right to privacy is not specifically mentioned by Roman jurists, several *injuriae* or affronts to personality which are very similar to the modern right were recognised.¹³⁵⁹ Personality interests are non-patrimonial interests that cannot exist separately from the individual.¹³⁶⁰ They come into existence with the birth of a human being, they cannot be inherited or attached and are incapable of being relinquished except at the death of a human being at which they are terminated.¹³⁶¹

¹³⁵⁸ Although South Africa has a Civil Law System, it is called the “common law”(gemenerereg) in South Africa. See for example Section 8(3)(b) and Section 39 of the Constitution of the Republic of South Africa (Act 108 of 1996).

¹³⁵⁹ D J McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 13.

¹³⁶⁰ Cf J Neethling *Persoonlikheidsreg* (1985) as cited in Anneliese Roos *The Law of Privacy (Data) Protection: A Comparative and Theoretical Study* (2003) at 545.

¹³⁶¹ Cf Roos op cit at 545.

The Roman law *actio injuriarum* forms the basis for the protection of personality rights in South Africa.¹³⁶² The modern *actio injuriarum* developed from the recognition and protection of specific wrongs under Roman law. It came about as a result of a gradual movement from specific wrongs to a general action.¹³⁶³

The *actio injuriarum* protected against wrongs against *corpus* (physical integrity), *fama* (good name) and *dignitas*.¹³⁶⁴ Although there are varied opinions as to the specific meaning of the concept of *dignitas*, it is generally regarded as a collective term for all personality interests excluding *corpus* and *fama*.¹³⁶⁵ For an action based on the *actio injuriarum* to succeed at common law, the elements of wrongfulness, intention and infringement must be proved.¹³⁶⁶ (In the case of the mass media, negligence, and not intention, must be proved.)¹³⁶⁷ Each of these elements will be discussed in more detail, after which the relevance of the *actio injuriarum* for the protection of privacy and data in Internet cafes will be considered.¹³⁶⁸

¹³⁶² *O'Keefe v Argus Printing & Publishing Co Ltd & Anor* 1954 3 SA 244, 248 (C) Cf D J McQuoid-Mason "Privacy" in M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz, S Woolman *Constitutional Law of South Africa* (2004) at 38-3. See also R G McKerron *The Law of Delict* 7 ed (1971) at 9.

¹³⁶³ See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 13ff.

¹³⁶⁴ Cf *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1979 (1) SA 441 (A). Cf Neethling *persoonlikheidsreg* 53 cited in Roos at 546.

¹³⁶⁵ Cf J Neethling, J M Potgieter and P J Visser *Law of Delict* (2006) 5th ed at 14.

¹³⁶⁶ Cf McQuoid-Mason in Chaskalson et al op cit at 38-3.

¹³⁶⁷ *Ibid.*

¹³⁶⁸ This approach has been adopted in this section because the chapter appeared fragmented and incohesive when the former method (where relevance to Internet cafes was discussed after each subtopic) was followed.

6.1.1. 1 Wrongfulness

For an action based on the *actio injuriarum* to be successful, the wrong had to be *contra bonos mores* – wrongful according to the prevailing *mores* of the society. The wrongfulness of a factual infringement of privacy is judged in the light of contemporary *boni mores* and the general sense of justice of the community as perceived by the court.¹³⁶⁹

In determining the current modes of thought and values of any community, the courts must have regard to the Constitution¹³⁷⁰ and may be influenced by its statute law.¹³⁷¹ The South African Constitution is bound to have a great influence in determining the new *boni mores* of the South African society.¹³⁷² In accordance with the provisions of the Constitution,¹³⁷³ the courts may also be influenced by developments in other legal systems.¹³⁷⁴ It has been pointed out however that tests of legal convictions and the *boni mores* of the community are seldom used, as the fact of an infringement of another's right is a primary indication of wrongfulness.¹³⁷⁵ Infringement alone however, is not sufficient to determine wrongfulness.¹³⁷⁶

¹³⁶⁹ *Financial Mail (Pty) Ltd & Others v Sage Holding Ltd & Another* 1993 (2) SA 451 (A) at 462G.

¹³⁷⁰ See *Gardener v Whitaker* 1995 (2) SA 672 (E).

¹³⁷¹ Cf *Rhodesian Printing and Publishing Co Ltd v Duggan & Another* 1975 (1) SA 590 (RA) at 595.

¹³⁷² See *Carmichelle v Minister of Safety and Security (Centre for Applied Legal Studies Intervening)* 2001 4 SA 938 (CC).

¹³⁷³ Section 39(1)c, Act 108 of 1996.

¹³⁷⁴ See *Bernstein v Bester NO* 1996 (2) SA 751 (CC); See above Para 1.5.

6.1.1.2 *Animus injuriandi* (Intention)

Traditionally, in order to be actionable, the act had to be done intentionally—with the intention to injure. The intention to injure refers to the direction of the wrongdoer’s will towards his or her conduct.¹³⁷⁷ Intention to injure will be presumed where the consequence or result of the wrongdoer’s action was his or her principal object or where he or she might have foreseen that those consequences or results would follow his or her action.¹³⁷⁸

Animus injuriandi includes the intention to injure and consciousness of wrongfulness.¹³⁷⁹

Consciousness of wrongfulness means that the defendant must know that his or her conduct is wrong.¹³⁸⁰ In *Dantex Investment Holdings (Pty) Ltd v Brenner*,¹³⁸¹ it was said: “It is now accepted that *dolus* encompasses not only the intention to achieve a particular result, but also the consciousness that such a result would be wrongful or unlawful.” In other words, the requirement of *animus injuriandi* is that the defendant’s action must be a

¹³⁷⁵ Neethling et al op cit at 45.

¹³⁷⁶ Ibid.

¹³⁷⁷ McQuoid-Mason in Chaskalson et al op cit at 38-4.

¹³⁷⁸ Neethling et al op cit at 15, 123f.

¹³⁷⁹ *Minister of Justice v Hofmeyr* 1993 (3) SA131 (A) at 154.

¹³⁸⁰ Neethling et al op cit at 117,119.

¹³⁸¹ 1989 (1) SA 390 (A), at 396 per Grosskopf J.A.

willed wrongful act. Once the other elements of an invasion of privacy have been proved, *animus injuriandi* will be presumed.¹³⁸²

For the mass media, negligence, not intention, must be proved,¹³⁸³ and the defences that negate wrongfulness or unlawfulness may be used.¹³⁸⁴ In this regard, the criterion of reasonableness is used to determine the unlawfulness of the act complained of.¹³⁸⁵ In the light of Section 16 of the Constitution, which guarantees freedom of expression, the courts have to weigh the right to privacy against the freedom of the press.¹³⁸⁶

6.1.1.3 Impairment of Privacy

An impairment of the plaintiff's privacy means that the plaintiff's *dignitas* has been hurt or damaged.¹³⁸⁷ In order to succeed the plaintiff has to show that his or her personality rights have been infringed, in this instance, the right to privacy. The interests of the right to privacy recognised and protected by the South African courts have been broadly classified as follows: Intrusions or interferences with private life, and disclosures and

¹³⁸² *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (C). See also *C v Minister of Correctional Services* 1996 4 SA 292 (T) at 304-305.

¹³⁸³ Cf *National Media Ltd v Bogoshi* 1998 (4) SA 1195 (SCA).

¹³⁸⁴ *Ibid* at 1213-1215, where the court held that the mass media may escape liability for defamation if they are not negligent. See also J Burchell *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum* (1998) at 223f.

¹³⁸⁵ Cf *National Media Ltd v Bogoshi* *supra*. Cf McQuoid-Mason in Chaskalson et al op cit at 38-5.

¹³⁸⁶ See generally McQuoid-Mason in Chaskalson et al op cit at 38-6. See also Cameron J in *Holomisa v Argus Newspapers Ltd* 1996 (2) SA 588 (W).

¹³⁸⁷ Cf Neethling et al op cit at 16; see also McQuoid-Mason *The Law of Privacy in South Africa* op cit at 27, McQuoid-Mason in Chaskalson et al op cit at 18-2.

acquisition of information.¹³⁸⁸ It has been contended that false light and appropriation cases, should not be classified as cases of invasions of privacy, but cases of wrongful infringement of identity.¹³⁸⁹

It is arguable that while identity and privacy are different concepts, they are not mutually exclusive concepts. A parallel may be drawn between data and privacy and identity and privacy as follows: While data protection may legally be distinguished from privacy protection,¹³⁹⁰ the interests protected by privacy and data laws may overlap and the concepts have been used interchangeably.¹³⁹¹ It is therefore suggested that if, for the purpose of clarity in legal argument, and ease of classification, false light and appropriation are regarded as cases of infringement of identity, they should not be, by that fact, altogether excluded from the ambit of privacy protection.

6.1.1.4 Relevance to Internet Cafes

To be relevant for the protection of privacy in Internet cafes, the essential components of the *actio injuriarum* which are: wrongfulness, intention and impairment of the plaintiff's *dignitas* must be proved. The requirement of wrongfulness will be satisfied where an act amounting to an invasion of privacy constitutes an infringement on another's rights as provided for by the Constitution or statute law. Thus, where privacy invasion in an

¹³⁸⁸ Cf McQuoid-Mason in Chaskalson et al op cit at 18-4.

¹³⁸⁹ Neethling et al op cit at 356ff. Cf J Neethling *Law of Personality* (2005) at 295.

¹³⁹⁰ Cf Neethling *Persoonlikheidsreg* as cited in Roos op cit at 544, 545.

Internet café involves an unlawful search, seizure or infringement on communication in violation of Section 14 of the South African Constitution,¹³⁹² there will be liability for such invasion. Similarly, where e-mail or telephonic communications transmitted in an Internet café is monitored or intercepted without complying with the provisions of the Interception and Monitoring (Prohibition) Act¹³⁹³ there will be liability in respect of such monitoring or interception.

The requirement for *animus injuriandi* refers to the intention to injure and looks at the consciousness knowledge of wrongfulness of the act. Once it has been proved that the act complained of amounts to a contravention of the Constitution and that the plaintiff has suffered some hurt, damage, loss or injury in respect of the invasion of privacy, *animus injuriandi* will be presumed and there will be liability unless the defendant can provide rebuttal.

As for the requirement for impairment of the plaintiff's *dignitas*, it will be sufficient in any Internet café invasion of privacy case to show that the plaintiff's personality rights have been infringed. Thus where there has been an intrusion or disclosure of information obtained through an Internet café in invading the plaintiff's privacy, action will lie against the defendant in respect of such intrusion or disclosure under the South African Common Law.

¹³⁹¹ Cf above Para 1.2.

¹³⁹² Act 108 of 1996.

In the absence of a clear cut Common Law right to privacy in Nigerian Internet café privacy cases, it is submitted that the constitutional guarantee of the right to privacy contained in Section 36¹³⁹⁴ may be relied on to prove an impairment of *dignitas*. Since Section 36 specifically provides for the protection of correspondence and telegraphic communication under which e-mail and other information processed via the Internet may be legally protected,¹³⁹⁵ it is submitted that violation of any of these rights may be regarded as impairment of *dignitas* for the purpose of establishing *animus iniuriandi* once wrongfulness and intention are present.

6.1.1.5 Case Law

The privacy interests protected by South African courts may also be classified more simply as protecting substantive privacy rights on the one hand, and disclosural privacy rights on the other.¹³⁹⁶ The following are some of the cases in which South African courts have protected the right to privacy.

In *De Fourd v Municipal Council of Cape Town*,¹³⁹⁷ the Cape Supreme Court held that illegal entry into a private residence constitutes a wrongful intrusion.¹³⁹⁸ In *S v A*,¹³⁹⁹ the court held that it was wrongful intrusion to electronically bug a person's home.

¹³⁹³ Act 127 of 1992. Cf below Para 7.1.2.1.2.

¹³⁹⁴ 1979 Constitution FRN.

¹³⁹⁵ Cf below Para 7.2.1.1.

¹³⁹⁶ *Ibid*; See also *Financial Mail Pty Ltd and Others v Sage Holdings Ltd and Another* supra at 462G.

In *S v Hammer & Others*,¹⁴⁰⁰ it was held that it was an intrusion to read the correspondence of another. It has also been held to be an intrusion to listen in to private conversations,¹⁴⁰¹ and to shadow a person.¹⁴⁰² In *Reid-Daly v Hickmann & Others*,¹⁴⁰³ the Zimbabwe Appeal Court held that the reading of private documents is an actionable intrusion. It has also been held to be actionable intrusion to secretly watch a person undress¹⁴⁰⁴ or bath.¹⁴⁰⁵

In *Financial Mail (Pty) Ltd. v Sage Holdings Ltd*,¹⁴⁰⁶ the court held that it was an actionable disclosure to publish information obtained by means of illegal telephone tapping. The act of telephone tapping was considered to be a wrongful act of intrusion in this case.

¹³⁹⁷ (1898) 15 SC 399 at 402.

¹³⁹⁸ See also *S v I and Another* 1976 (1) SA 781 (RA); *S v Boshoff and Others* 1981 (1) SA 393 (T) at 396.

¹³⁹⁹ *Supra*.

¹⁴⁰⁰ 1994 (2) SACR 496 (C) at 498.

¹⁴⁰¹ *S v A and Another* 1971 (2) SA 293 (T). See also *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* *supra* (n 96 at 463).

¹⁴⁰² *Epstein v Epstein* 1906 TH 87.

¹⁴⁰³ 1981 (2) SA 315 (ZA) at 323. Zimbabwe has a Roman-Dutch law system and its decisions may be of persuasive value.

¹⁴⁰⁴ *R v Holliday* 1927 CPD 395 at 401; *R v Daniels* 1938 TPD 312 at 313.

¹⁴⁰⁵ *R v Schoonberg* 1926 OPD 247.

¹⁴⁰⁶ *Supra*.

In *O'Keefe v Argus Printing and Publishing Co Ltd*,¹⁴⁰⁷ the plaintiff was a well-known radio announcer who allowed herself to be photographed to illustrate a news story. The photograph was subsequently published as an advertisement for firearms without her consent. The court held that the publication was an aggression upon the plaintiff's *dignitas*, actionable under the *actio injuriarum*. Similarly, where the plaintiffs' photograph was used for a false newspaper story without their consent, it was held to be an actionable disclosure.¹⁴⁰⁸

In *Mhlongo v Bailey & Another*,¹⁴⁰⁹ the unauthorised publication of a photograph of a retired schoolteacher portraying him as a young man in the company of a well-known singer was held to be an actionable intrusion. In *Rhodesian Printing and Publishing Co Ltd v Duggan*¹⁴¹⁰ the publication of a story about young children abducted from the custody of their parents the defendants was held to be an actionable disclosure.

Similarly in *National Media Ltd & Another v Jooste*,¹⁴¹¹ the defendants were held liable for the unauthorised publication of a photograph and story about an unmarried mother who conceived a child by a well-known rugby player.

¹⁴⁰⁷ 1954 (3) SA 244 (C).

¹⁴⁰⁸ *Kidson v SA Associated Newspapers Ltd* supra.

¹⁴⁰⁹ 1958 (1) SA 370 (W).

¹⁴¹⁰ 1975 (1) SA 590 (RA).

¹⁴¹¹ 1996 (3) SA 262 (A) at 271.

Where the plaintiff's action succeeds, he or she will be awarded damages, or may obtain an interdict restraining a proposed or continued invasion of privacy.¹⁴¹² The plaintiff may also obtain both an award of damages and an interdict.¹⁴¹³

It has also been held that the disclosure of private facts contrary to the existence of a confidential relationship is actionable.¹⁴¹⁴

6.1.1.5a Relevance to Internet Cafes

South African Common Law privacy cases will be apt for the protection of privacy in Internet cafes. The intrusion cases will be relevant for imposing liability in respect of unlawful entry as well as unlawful access to information in Internet cafés. Thus, where there is an unlawful entry on Internet café premises to obtain information, there will be liability for the unlawful entry. Also, where information is unlawfully obtained by means of an unlawfully entry on Internet café premises, both the entry and the unlawful obtaining of information will constitute intrusions for which there will be liability.

¹⁴¹² *Epstein v Epstein supra*; *Rhodesian Printing and publishing Co Ltd v Duggan supra*; *Financial Mail Pty Ltd v Sage Holdings (Ltd) supra*. See generally E. Newman & DJ McQuoid-Mason (eds.) *The South African Law of Obligations* (1978) at 349.

¹⁴¹³ See *Stellenbosch Wine Trust Ltd v Oude Meester Group Ltd* 1972 (3) SA 152 (C) 161f. Cf Newman & McQuoid-Mason op cit at 349. However, interdicts have become difficult to obtain because of Section 16 of the Constitution, which provides for freedom of expression; See *Mandela v Falati* 1995 (1) SA 251(W) 257.

¹⁴¹⁴ *Jansen van Vuuren NO v Kruger* 1993 (4) SA 842 (A). Cf Neethling et al op cit at 334.

There will also be liability for intrusion in respect of the reading of another's e-mail correspondence or other personal information processed through the Internet. As between Internet café personnel and their customers, it is submitted that it will *prima facie* constitute an intrusion for an Internet café owner, or his/her staff to access the contents of a client's e-mail without the client's consent or other lawful justification. Where however there is a need to access the client's e-mail for instance, at the request of the client, or in the course of updating the computer system, a duty of confidence should be imposed on the Internet café owner or licensee and his/her staff regarding disclosure of the information so accessed.¹⁴¹⁵

South African Common Law cases on disclosure will be relevant for the protection of privacy in Internet cafes where information is unlawfully published or disclosed to another. There will be liability for disclosure where the information that was published was sourced from an Internet café as well as, where such information was published by means of equipment in an Internet café. Thus, the unauthorised publication of personal information, photographs or contents of e-mail correspondence obtained from computers in Internet cafes will be actionable.

6.1.1.6 Defences

There are certain defences open to a defendant when there has been an invasion of privacy. The defendant may escape liability by relying on one or more of the following

¹⁴¹⁵ Cf *Jansen van Vuuren NO v Kruger* 1993 (4) SA 842 (A). Cf Neethling et al op cit at 334.

defences negating unlawfulness: justification, fair comment, privilege, consent, necessity, private defence and statutory authority. He or she may also raise defences excluding intention such as mistake, intoxication or insanity.¹⁴¹⁶

6.1.1.6.1 Defences Negating Unlawfulness

6.1.1.6.1.1 Justification

The defence of justification will avail the defendant where the disclosures made about the plaintiff are true and in the public interest (for example where the plaintiff is a public figure).¹⁴¹⁷ The essence of justification is that the statements made were true and that they were of public benefit.¹⁴¹⁸ It has been said that in cases of invasions of privacy arising from publication of private facts and in false light cases, the defendant may rely on the defence of justification to avoid liability.¹⁴¹⁹

6.1.1.6.1.1a Relevance to Internet Cafes

¹⁴¹⁶ See generally McQuoid-Mason in Chaskalson et al op cit at 18-6 & 18-7.

¹⁴¹⁷ *Jooste v National Media Ltd* 1994 (2) SA 634 (C) at 645. See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 218-224. Cf Neethling *Law of Personality* op cit at 276 and Burchell op cit at 476, who are of the opinion that the defence of truth for the public benefit does not to apply to invasion of privacy cases. However, in *Jansen van Vuuren & Another v Kruger* 1993 (4) SA 842 (A), the court established that that the defamation defences may also be used in cases of invasion of privacy (at 350). See further McQuoid-Mason in Chaskalson et al op cit at 38-13.

¹⁴¹⁸ Ibid. Cf *S v I & Another* 1976 (1) SA 781 (RA).

¹⁴¹⁹ McQuoid-Mason *The Law of Privacy in South Africa* op cit at 224.

This defence may leave a leeway for Internet café personnel and others in cases involving the publication or disclosure of personal information about customers, since information published, if sourced from the plaintiff's records, will generally be true.¹⁴²⁰ However, publication must also be in the public interest to be justified. It is submitted in this regard, that, if a distinction is drawn between “matters of public interest” and “matters of interest to the public”, as in the United Kingdom,¹⁴²¹ this will significantly narrow the margin for reliance on the defence of justification in Internet café privacy cases in Nigeria.

The defence of justification will not avail a defendant where it is proved that he or she acted out of malice or spite.¹⁴²²

6.1.1.6.1.2 Fair Comment

This defence is available in false light invasion of privacy cases. It may be raised where the statement made by the defendant is a comment, and not a statement of fact; the comment made is fair; the facts commented on are true and the comment¹⁴²³ or the statement is made on a matter of public interest.¹⁴²⁴ As in the case of justification, this defence will not be successful if the plaintiff can show malice or improper motive on the part of the defendant.¹⁴²⁵ In cases of disclosure, the defence will succeed where

¹⁴²⁰Cf *National Media Ltd v Bogoshi* supra. Cf the United Kingdom's position in *Mrs R v Central Television* [1994] Fam 192), and the position in the United States in *Mcnamara v Freedom Newspapers* (1991) Tex App Corpus Christi 802 SW 2d 901. It appears that the defence of public interest often avails the media. Cf Roos op cit at 599 who asserts that privacy can only be infringed by the publication of true information.

¹⁴²¹ Cf *Lion Laboratories v Evans* [1985] 1 QB 526 at 537 Cf above Para 3.2.2.1.1.1.

¹⁴²² *Coetzee v Nel* 1972 (1) SA 353 (A) 374 See also *Jansen van Vuuren v Kruger* supra. See generally Newman & McQuoid-Mason op cit at 332.

publication is in the public interest. Thus, where, for instance, in commenting about a trainee or student, in a letter of reference, a tutor discloses personal information about the student, the defence of fair comment will avail the tutor.

6.1.1.6.1.2a Relevance to Internet Cafes

Where information disclosed or published about an Internet café user amounts to a fair assessment based on true facts relating to his/her Internet café practice, or, where such publication is in public interest, the defence of fair comment may avail the defendant.

Thus, where for instance, based on observation and documentation of the fact that an Internet café customer constantly and consistently daily watches pornographic material on the Internet, an Internet café owner says that such customer is obsessed with sex, the defence of fair comment will avail the Internet café owner.

6.1.1.6.1.3 Necessity

¹⁴²³ See *Johnson v Beckett* 1992 (1) SA 762 (A) at 780-781.

¹⁴²⁴ Cf *McQuoid-Mason in Chaskalson et al op cit* at (18-6); See also *Neethling et al op cit* at 347.

¹⁴²⁵ *Marais v Richard* 1981 (1) SA 1157 (A) 1170.

This defence is available “where the defendant has acted reasonably to prevent a threat of greater harm to another person arising from force of nature or conduct unconnected with the plaintiff”¹⁴²⁶ and may be applied in cases of intrusions, publication of private facts and false light cases.¹⁴²⁷ The defence of necessity will apply for instance in the case of shops with closed circuit television systems.¹⁴²⁸

6.1.1.6.1.3a Relevance to Internet Cafes

The defence of necessity will be relevant where, for example, surveillance devices are installed in Internet cafes for the security purposes.

6.1.1.6.1.4 Consent

Where the plaintiff has given consent to the action complained of, the defendant may successfully raise this defence, provided that the defendant acts within the limit of the consent given.¹⁴²⁹ This is based on the principle of *volenti non fit injuria*¹⁴³⁰ and it has been pointed out that consent would be “a good defence to all forms of invasions.”¹⁴³¹ It

¹⁴²⁶ McQuoid-Mason *The Law of Privacy in South Africa* op cit at 233. *Rhodes University College v Field* 1947 (3) SA 437 (A) at 463.

¹⁴²⁷ See McQuoid-Mason *The Law of Privacy in South Africa* op cit at 233.

¹⁴²⁸ See Burchell op cit at 424.

¹⁴²⁹ See *Kidson v SA Associated Newspapers Ltd* supra, *O’Keefe v Argus Printing & Publishing Co Ltd* supra. See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 231.

¹⁴³⁰ See generally McQuoid-Mason *The Law of Privacy in South Africa* at 231.

¹⁴³¹ Cf McQuoid-Mason op cit at 232.

has also been established that the defence of consent will only avail a defendant where the plaintiff had “knowledge, appreciation and consent” concerning the invasion by the defendant.¹⁴³²

Consent may be express or implied.¹⁴³³ Thus, for example, where a person willingly joins an organisation that is known to request the disclosure of personal information from, and sharing of such information amongst, its members, he or she will be deemed to have given consent to any disclosure of personal information regarding himself or herself to other members of that organization.

6.1.1.6.1.4a Relevance to Internet Cafes

This defence will be available to Internet café personnel where, at the customers’ requests, they check e-mail on their behalf or download other information. It will also apply where in the process of assisting customers, Internet café personnel come into contact with personal information relating to customers. However, it is submitted that where a client authorises an Internet café owner to check mail or download material on his/her behalf or to otherwise assist, even where there is consent in respect of access to such mail or other information, an Internet café owner will be liable for any unlawful use of such information, for having acted outside the limits of the consent given.¹⁴³⁴

¹⁴³² *Waring & Gillow Ltd v Sherborne* 1904 TS 340 at 344.

¹⁴³³ Cf McQuoid-Mason *The Law of Privacy in South Africa* op cit at 231; See generally Newman & McQuoid-Mason op cit at 265.

6.1.1.6.1.5 *Statutory Authority*

This defence serves to legalise acts of the defendant (in this case, invasions of privacy) which would otherwise be unlawful.¹⁴³⁵ For instance, the Criminal Procedure Act¹⁴³⁶ contains a number of provisions conferring powers of search and seizure on police officials.¹⁴³⁷ Section 37 also provides for the taking of fingerprints of accused persons.¹⁴³⁸ The statutes concerned must however not be violations of any constitutional provision.

In *Mistry v Interim National Medical and Dental Council of South Africa and others*,¹⁴³⁹ the Constitutional Court declared a section of an Act¹⁴⁴⁰ which empowered inspectors to enter and search premises without a warrant and to seize medicines to be inconsistent with the right to privacy guaranteed by the Constitution. As such, the defence of statutory authority will not be available where a search or seizure that would amount to an invasion of privacy is purportedly carried out under these provisions.

¹⁴³⁴ Cf *Kidson v SA Associated Newspapers Ltd* supra; *O'Keefe v Argus Printing & Publishing Co Ltd* supra; *Jooste v National Media Ltd* supra.

¹⁴³⁵ In *S v Human & Another* 1996 (1) SA 232 (W) at 233, 237, the taking of fingerprints of an arrested person pursuant to section 37 of the Criminal Procedure Act was found not to be unlawful (although in this case, the question of privacy was not raised). See also *Jooste v National Media Ltd* supra.

¹⁴³⁶ Act 51 of 1977.

¹⁴³⁷ Generally Chapter 2, specifically, sections 19-25.

¹⁴³⁸ *S v Human* supra

¹⁴³⁹ 1998 (7) BCLR 880 (CC).

6.1.1.6.1.5a Relevance to Internet Cafes

Where an Internet café owner, Internet cafe personnel, or any other person is required by law to disclose any information processed in Internet cafes relating to others and subsequently does so, the defence of statutory authority will be available in respect of such disclosure.

6.1.1.6.1.6 *Private Defence*

Where reasonable force is used to repel an immediate attack on the person or property of the defendant, or of another, where such an attack is caused by the plaintiff or his or her property, the defendant will not be liable for the attack.¹⁴⁴¹ This defence may be construed for the protection of a defendant where files or messages are inspected, deleted or destroyed to prevent viruses introduced or caused by the plaintiff's document.

6.1.1.6.1.6a Relevance to Internet Cafes

This defence will avail Internet café personnel where information contained in Internet café computers is deleted or destroyed in order to debug the computers or salvage their hard drive from corruption caused by the plaintiff's document. It will also be available where Internet café personnel access and check e-mail messages or other files of customers in order to prevent or treat viruses.

¹⁴⁴⁰ Medicines and Related Substances Control Act 101 of 1965, Section 28(1).

6.1.1.6.1.7 *Absolute Privilege*

Absolute privilege applies in South African law¹⁴⁴² in specific instances, to statements made in the course of debates or proceedings before Parliament,¹⁴⁴³ or the provincial councils.¹⁴⁴⁴ Proof of malice on the part of the defendant will not defeat a defence of absolute privilege.¹⁴⁴⁵ For instance, where a member of parliament discloses personal information about another in the course of parliamentary proceedings, that would ordinarily constitute an infringement of privacy, the defence of absolute privilege will justify the infringement.

6.1.1.6.1.7a Relevance to Internet Cafes

This defence will be of little or no practical relevance for the processing of information in Internet cafes.

6.1.1.6.1.8 *Qualified Privilege*

¹⁴⁴¹ See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 234.

¹⁴⁴² Cf Stratford CJ in *Sather v Orr* 1938 AD 426. See generally Newman & McQuoid-Mason op cit at 335.

¹⁴⁴³ Sections 2 & 8, Powers and Privileges of Parliament Act 91 of 1963.

¹⁴⁴⁴ Section 1A Powers and Privileges of Provincial Councils Act 16 of 1948.

¹⁴⁴⁵ See Newman & McQuoid-Mason op cit at 334 f; McQuoid-Mason *The Law of Privacy in South Africa* op cit at 225.

Where the plaintiff's privacy is invaded in the discharge of a duty by the defendant, or on an occasion when the defendant was entitled to do so in the exercise of a right, the defence of privilege will be available.¹⁴⁴⁶ The defence of qualified privilege will avail a defendant where the defendant has "a legal, moral or social duty to speak or a legitimate interest to protect" and the listener has a corresponding interest to receive it.¹⁴⁴⁷ The information disclosed must however be relevant to the purpose being served, or reasonably connected to it.¹⁴⁴⁸

Where a teacher discloses confidential facts about a student to the student's parents or legal guardians, the defence of qualified privilege will avail the teacher. The defence of qualified privilege also works in connection with public interest, for instance where the media in the exercise of their duty publish information or reports in the public interest.¹⁴⁴⁹ For the mass media, the criterion of "reasonableness" is also used to prove lack of negligence and thus rebut fault.¹⁴⁵⁰ Reasonableness may also be used in determining the wrongfulness of the act, to rebut unlawfulness.¹⁴⁵¹

¹⁴⁴⁶ See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 224. In *Mistry v Interim National Medical & Dental Council of South Africa & others* 1998 (7) BCLR 880 (CC), where information was obtained in circumstances analogous to a privileged occasion, the obtaining of information was held not to constitute an invasion of privacy. (McQuoid-Mason op cit).

¹⁴⁴⁷ See *Lappan v Corporation of Grahamstown* 1906 EDL 41. Cf *Davis v Additional Magistrate, Johannesburg, and Others* 1989 (4) SA 299 (W) at 303E-1; *Jansen van Vuuren v Kruger* supra.

¹⁴⁴⁸ Cf Roos op cit at 600.

¹⁴⁴⁹ Cf *National Media Ltd v Bogoshi* supra. See also McQuoid-Mason *The Law of Privacy in South Africa* op cit at 225ff.

¹⁴⁵⁰ See *National Media Ltd v Bogoshi* supra. Cf McQuoid-Mason in Chaskalson et al op cit at 38-16.

¹⁴⁵¹ Cf *Bogoshi* supra. See also Burchell op cit at 227; McQuoid-Mason in Chaskalson et al op cit at 38-16.

Certain reports of parliamentary¹⁴⁵² or judiciary proceedings¹⁴⁵³ are also covered by qualified privilege.¹⁴⁵⁴ Proof of malice may however defeat the defence of qualified privilege.¹⁴⁵⁵

It must be noted that there is no closed list of defences negating wrongfulness.¹⁴⁵⁶

6.1.1.6.1.8a Relevance to Internet Cafes

This defence will be available where, for instance, an Internet café user's privacy is invaded as a result of the disclosure by an Internet café owner or worker of information processed in an Internet cafe, under circumstances in which the Internet café owner/worker is under a legal or moral duty to speak. For example, where information gathered in an Internet café from another's e-mail or Internet records about a fraud ring or about the planned commission of a crime is disclosed to law enforcement agents or where an Internet cafe owner or staff is subpoenaed to give evidence concerning the plaintiff.

6.1.1.6.2 Defences Excluding Intention

¹⁴⁵² *Hearson v Natal Witness Ltd* 1935 NPD 603 at 605.

¹⁴⁵³ *Van Leggelo v Argus Printing & Publishing Co Ltd* 1935 TPD 230 at 237ff.

¹⁴⁵⁴ See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 225ff.

¹⁴⁵⁵ *Basner v Trigger* 1946 AD 83 at 93f.

¹⁴⁵⁶ Cf *Muller v SA Associated Newspapers Ltd* 1972 (2) SA 589 (C) at 592.

The categories of defences available to exclude intention are not closed,¹⁴⁵⁷ and may be used where it can be shown subjectively that the defendant did not intend to injure the plaintiff, for example, in cases involving intoxication or insanity. Others are mistake, jest and *rixa*. The element of consciousness of wrongfulness is absent in such cases.¹⁴⁵⁸ It has been contended that in view of the importance of the constitutional right to privacy, “the defence of *bona fide* unconsciousness of wrongfulness should not be available to the defendant unless it is also reasonable.”¹⁴⁵⁹

6.1.1.6.2.1 Intoxication

The defence of intoxication will be available in respect of an invasion of privacy where a person acting under the influence of alcohol invades another’s privacy. For example, where the defendant, being inebriated, discloses personal or confidential information about another (e.g. that the other has a secret dreaded disease)¹⁴⁶⁰ or peeps through the window of another, the defence of intoxication will be available in respect of the disclosure or intrusion.

6.1.1.6.2.1a Relevance to Internet Cafes

¹⁴⁵⁷ Cf *Geyser en 'n ander v Pont* 1968 (4) SA 67 (W) at 72-3. See generally McQuoid-Mason op cit at 236ff.

¹⁴⁵⁸ Cf Roos op cit at 624.

¹⁴⁵⁹ McQuoid-Mason in Chaskalson et al op cit at 38-13.

¹⁴⁶⁰ *Muller v SA Associated Newspapers Ltd* supra at 592.

This defence will be available to Internet café personnel as well and third parties where they access or disclose personal information concerning another processed in an Internet café when they are under the influence of alcohol. The Internet cafe owner, worker or other person will be able to rely on the defence of intoxication in respect of such intrusion or disclosure.

6.1.1.6.2.2 *Insanity*

The defence of insanity will also avail a defendant, to rebut consciousness of wrongfulness, where he or she, discloses personal information about another, commits an act of intrusion or appropriation, or places the plaintiff in a false light in circumstances the defendant can be proved to have been insane.¹⁴⁶¹

6.1.1.6.2.2a Relevance to Internet Cafes

The defence of insanity, like intoxication, will be open to all categories of Internet café users in respect of any act amounting to an invasion of privacy viz: intrusions, disclosure, false light and appropriation. Where, for instance, the plaintiff's privacy is invaded by the defendant's unlawful reading of the plaintiff's correspondence or unauthorised publication of personal information processed in an Internet café, the defendant may rely on the defence of insanity to deny consciousness of wrongfulness.

¹⁴⁶¹ Cf *Wilhelm v Beamish* (1894) 11 SC 13 at 15. See also *Muller v SA Associated Newspapers Ltd* supra at 592.

6.1.1.6.2.3 *Mistake*

The defence of mistake will be available where the defendant had no intention to invade the privacy of the plaintiff, or was *bona fide* unaware that his or her act was wrongful.¹⁴⁶²

For instance, where personal information regarding an employee, contained in an office computer is inadvertently sent to another in the course of business, by the secretary, the defence of mistake will avail the secretary. However, if the mistake arose out of the defendant's carelessness or recklessness, then there will be *dolus eventualis* and the defendant will be held liable for the mistake.

6.1.1.6.2.3a **Relevance to Internet Cafes**

This defence will be useful for the protection of Internet cafe personnel where in the course of assisting customers, information regarding other customers is inadvertently disclosed to other customers. For example, where an Internet café owner inadvertently gives downloaded mail or information to another customer, for whom it is not intended.

6.1.1.6.2.4 *Jest*

The defence of jest will be available to the defendant where he or she publishes information, or commits an act of intrusion, or otherwise invades a person's privacy as a

¹⁴⁶² *Maisel v Van Naeren* 1960 (4) SA 836 (C). Cf *McQuoid-Mason* in *Chaskalson et al op cit* at 38-17.

joke.¹⁴⁶³ For example, where, a group of young boys are jesting in a bar and one of them, in the course of joking about their sexual activities, jokingly discloses personal information regarding the sexual activities of another friend who is present, the defence of jest will be available in respect of the disclosure.

6.1.1.6.2.4a Relevance to Internet Cafes

In line with the assertion that the availability of the defence of unconsciousness of wrong be restricted,¹⁴⁶⁴ it is affirmed that in the absence of strict restrictions, there is a potential for the misuse of this defence as a blanket excuse to avoid responsibility for reckless intrusions or disclosures. It will thus be suggested for our purpose that the defence of jest should only be applicable where the plaintiff and defendant have a somewhat informal or personal relationship. Thus, Internet café personnel will ordinarily be excluded from raising the defence if they only have a business relationship with the customer. The defence will however be available as between friends or business colleagues where jokes containing personal information are sent via e-mail.

6.1.1.6.2.5 *Rixa*

The defence of *rixa* will be available where the plaintiff's privacy is invaded by defamatory words uttered "without premeditation, in sudden anger on provocation by the

¹⁴⁶³ See generally McQuoid-Mason *The Law of privacy in South Africa* op cit at 236ff.

¹⁴⁶⁴ Cf McQuoid-Mason in Chaskalson et al op cit at 38-13 above at Para 6.1.1.6.2.

plaintiff, and the defendant did not subsequently persist in them.”¹⁴⁶⁵ For instance, where the defendant is subjected to constant ridicule by the plaintiff, and provoked by the plaintiff’s ridicule on a given occasion, the defendant, makes a statement regarding the plaintiff’s HIV positive status, but does not repeat the disclosure, the defence of *rixa* will avail the defendant.

6.1.1.6.2.5a Relevance to Internet Cafes

Again, it is doubtful whether Internet café personnel are in a position to rely on this defence considering the nature of their relationship with customers. For practical purposes, it is expected that Internet café personnel will maintain a business relationship and not be in a situation where they exchange words with customers. Where however, other persons who have come into contact with personal information processed in an Internet cafe discloses such information in the heat of provocation aroused by the plaintiff and does not persist thereafter with the disclosure, the defence of *rixa* will be available with respect to that disclosure.

There are doubts as to whether juristic persons can claim personality rights under the South African Common Law. While some courts have held that a juristic person have no right to privacy,¹⁴⁶⁶ there is authority to support the recognition of a confidential sphere that corporations or juristic persons have which the law may protect.¹⁴⁶⁷

¹⁴⁶⁵ See *Geysers v Pont* supra at 73; *Muller v SA Associated Newspapers Ltd* supra at 592. See generally Newman & McQuoid-Mason op cit at 342.

6.1.2 Common Law Protection of Data

Flowing from the above, data protection will be available at Common Law in cases of intrusion, unlawful publication, false light and appropriation. In this regard, there will be liability for unauthorised access to or, collection of information.¹⁴⁶⁸ Also, where information concerning an individual is wrongfully released by another, the former will be able to bring an action successfully if he or she can prove that the information was private and disclosed unlawfully,¹⁴⁶⁹ placed him or her in a false light,¹⁴⁷⁰ was used for

¹⁴⁶⁶ *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1979 (1) SA 441 (A) 453-4; *Boka Enterprises (Pvt) Ltd v Manatse* 1990 (3) SA 626 (ZH); *Church of Scientology in South Africa Incorporated Association Not for Gain v Readers Digest Association (SA) (Pty) Ltd* 1980 (4) SA 313 (C) 317-8; *AAIL (SA) v Muslim Judicial Council (Cape)* 1983 (4) SA 855 (C) 865.

¹⁴⁶⁷ *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another supra*; *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A). See also *Dhlomo v Natal Newspapers (Pty) Lt*, 1989 (1) SA 945 (A) Cf Neethling *Law of Personality* op cit at 295.

¹⁴⁶⁸ Cf Neethling *Law of Personality* at 298 where he states: "...the unauthorised collection or storage of personal information is in principle *contra bonos mores* and thus *prima facie* wrongful."

¹⁴⁶⁹ *Mhlongo v Bailey supra*, where the court upheld the principle that a person's past history is private. See also *Rhodesian Printing and Publishing Co Ltd v Duggan supra*. Cf Neethling *Law of Personality* op cit at 298 ff.

¹⁴⁷⁰ *Pickard v SA Trade Protection Society* (1905) 22 SC 89, where a credit bureau falsely published in a trade protection magazine that a person had had a provisional judgement taken against him. See also *Mangaroo v Toolsee* (1927) 48 NLR 100. Cf Neethling *Law of Personality* op cit at 299.

appropriation purposes,¹⁴⁷¹ that an action lay for defamation,¹⁴⁷² or that the disclosure or misuse of information constituted a breach of contract.¹⁴⁷³

Other than in these instances, however, there is no separate delict or distinct cause of action that solely protects data.

6.1.2a Relevance to Internet Cafes

South African Common Law will provide data protection with regard to information processed in Internet cafes where the act amounting to data infringement constitutes an intrusion, unlawful disclosure or where the use of the data places the plaintiff in a false light or constitutes appropriation. Thus there will be liability for unlawfully access to and/or disclosure of data where, for example, personal information stored in computers in an Internet café is unlawfully downloaded on to a disc, flash drive or any other copying device and published by Internet café personnel or a third party.

Liability will also lie in respect of the unlawful storage of the information in whatever form (floppy disc, flash drive e.t.c) employed by the defendant. Similarly, there will be

¹⁴⁷¹ In *O'Keefe v Argus Printing and Publishing Co Ltd* supra, where the plaintiff had consented to being photographed to illustrate a story, the pictures were improperly used for an advertisement, and the defendants' act was held to be an actionable disclosure. Similarly, where the use of data is not compatible with the purpose for which it was collected or otherwise improperly used, this will constitute an actionable disclosure. See also *Kidson v SA Associated Newspapers Ltd* supra. Cf Neethling *Law of Personality* op cit at 299.

¹⁴⁷² *Pickard v SA Trade Protection Society* supra; *Jooste v National Media Ltd* supra; *Mangaroo v Toolsee* supra. See also *Knoeson v Theron* 1904 (21) SC 177 at 181. Cf Neethling *Law of Personality* op cit at 295.

¹⁴⁷³ *Goodman v Von Molke* 1938 CPD 153. See Centlivres J at 157, where he observed that, "it is actionable to communicate information in breach of an agreement not to do so".

liability for unlawful access to or disclosure of data contained in customers' e-mail communication.

6.1. 3 Conclusion on Common Law Protection of Privacy and Data in South Africa

From the foregoing, it is clear that under South African Common Law, there is recognition of privacy rights. The classical *actio injuriarum* provided general protection against 'any vexatious violation of another person's rights.'¹⁴⁷⁴ From the cases, it is clear that this broad categorisation covered the interests protected by the law of privacy generally and can be applied to electronic mail and Internet usage specifically.

Although the technological revolution was still centuries away and many of the threats to privacy that now exist were absent in Roman times, it may be said that the foundations for a law of privacy already existed in Roman times.¹⁴⁷⁵ From the cases, there is no doubt that South African Common Law provides protection for the right to privacy with respect to both substantive and informational privacy rights.

The fact that the courts consider the contemporary *boni mores* in the light of the Constitution,¹⁴⁷⁶ and are also influenced by developments in other legal systems in determining the requirement of wrongfulness, effectively allows the law to change as

¹⁴⁷⁴ See generally McQuoid-Mason *The Law of Privacy in South Africa* op cit at 24-25.

¹⁴⁷⁵ Cf McQuoid-Mason op cit at 26-27.

times and moral values change.¹⁴⁷⁷ This flexibility enhances growth and development in the law, which is essential in contemporary times, and for our purposes, makes it possible to accommodate and offer protection for invasions of privacy relating to electronic mail and Internet use in cyber cafes. However, in all cases, the Common Law must be interpreted in the light of the Constitution.¹⁴⁷⁸

Limited protection can be found for data under the Common Law through the principles of the law of privacy and defamation. However, Common Law protection of data does not adequately cover present day data protection needs. The *lacuna* in the area of Common Law protection of data can probably be explained by the fact that the threat of abuse of data was not serious in Roman times. In any event, until the late 1970s data collection was done mostly by the state and its agencies, and the *actio injuriarum* provided sufficient protection for other types of affronts to a person's personality or dignity.¹⁴⁷⁹

However, today, public and private bodies, businesses and most, if not all, organisations, maintain records that may be classified as data.¹⁴⁸⁰ Where a person patronises a particular Internet café to send or receive mail or surf the Internet regularly, there will also be a

¹⁴⁷⁶ See *Gardener v Whitaker* supra.

¹⁴⁷⁷ See also *McQuoid-Mason* op cit at 118.

¹⁴⁷⁸ Cf *McQuoid-Mason* in *Chaskalson et al* op cit at 38-2.

¹⁴⁷⁹ See *McQuoid-Mason* op cit at 26 & 27.

¹⁴⁸⁰ Cf *Neethling Law of Personality* op cit 291-294.

substantial amount of personal information available on the computer system regarding them, which may be accessed by other people.

To respond to the modern day proliferation of technology facilitating access to personal information, the Promotion of Access to Information Act was enacted to provide for access to public and private records and generally regulate access to information in South Africa.¹⁴⁸¹ The provisions of the legislation will however be discussed in the next chapter, together with the constitutional right to privacy.¹⁴⁸²

6.1.3a Relevance to Internet Cafes

In the light of the above cases, it is clear that under the South African Common Law, unless the defendant can successfully raise one of the available defences, there will be liability for an invasion of privacy where there has been an intrusion, unlawful acquisition or disclosure of personal information.¹⁴⁸³ The applicability of different aspects of the South African Common Law for the protection of privacy and data in Internet cafes has also been shown. In this regard, it may be submitted that the South African Common law offers functional guidelines for the protection of privacy and data protection in Nigerian Internet cafes. The Nigerian Common Law privacy and data protection will now be examined.

¹⁴⁸¹ No 2 of 2000.

¹⁴⁸² See chapter 5.

¹⁴⁸³ *Financial Mail (Pty) Ltd v Sage Holdings Ltd* supra. Cf Neethling et al op cit at 356.

6.2 Common Law Protection of Privacy and Data in Nigeria

6.2. 1 Common Law Protection of Privacy

Prior to colonisation, Nigeria was a large geographical location with different peoples of diverse language and culture, who lived around The Niger area. At that time, the different people groups were each governed by traditional rulers amongst their indigenous peoples in accordance with their particular cultures. As such, there was no singularly applicable law or body of laws that could properly be called Common Law at the time.

Following the amalgamation and colonisation of Nigeria as it is known today, English law was applied in Nigeria by the colonial masters. After its independence in 1960, the English Common Law of England, the rules of Equity together with the Statutes of General Application in force in England on the 1st day of January 1900, were received and enacted into Nigerian law via different statutes operating in the then different regions of Nigeria.¹⁴⁸⁴ Thus, the adopted Common Law of England became the Common Law of Nigeria, and the English law of torts became the basis of the law of torts in Nigeria.¹⁴⁸⁵ In addition to the general reception of English Common law and Equity, legislation was also introduced in the different regions of Nigeria based on English enactments.¹⁴⁸⁶

¹⁴⁸⁴ See Section 45 Interpretation Act; Now cited as Cap 192 LFN 1990. See also D Olowu & F Laosebikan "Sources of Law in Nigeria" in A O Sanni (ed) *Introduction to Nigerian Legal Method* (1999) at 245-247.

¹⁴⁸⁵ Ibid.

¹⁴⁸⁶ For example the Defamation Law 1961 (Cap 34, Laws of Lagos State 1973), the Law Reform (Torts) Law 1961 (Cap 67, Laws of Lagos State 1973). See G Kodilinye *The Nigerian Law of Torts* (1982) at 11.

In effect, although decisions of foreign legal systems including England are generally not binding on Nigerian courts, but are of persuasive import,¹⁴⁸⁷ English Common Law and equitable doctrines¹⁴⁸⁸ have been incorporated into Nigerian law and constitute binding authority in the determination of relevant Nigerian cases.

As such, English Common Law remains not only relevant, but indispensable in the determination of Nigerian tort law cases and will feature significantly in the following paragraphs. In accounting for the reliance on English law, it must also be pointed out here that certain areas of the received English Common Law have not been the subject of much or any litigation in Nigeria.¹⁴⁸⁹ This will be reflected in the discussion of such areas of law where only the available English case law will be cited.

The same categories that were used to analyse the English law cases will be used in examining the Nigerian approach to privacy violations. The available provisions on the equitable action for breach of confidence will be examined first. The following torts will then be considered:

(a) trespass to person

¹⁴⁸⁷ Olowu & Laosebikan in Sanni op cit at 126. Cf Kodilinye op cit at 10 & 11.

¹⁴⁸⁸ It is noteworthy that the courts have construed the Interpretation Act as importing the English Common Law and doctrines of equity without applying the 1900 time constraint specified in the statute to the first half of the provision. Cf J O Asein *Introduction to Nigerian Legal System* (1998) at 102. See also Laosebikan and Olowu in Sanni op cit at 247.

¹⁴⁸⁹ Cf Reed J. in *The Queen v Bartholomew Princewell* (1963) 2 All NLR 31 at 31 where he observed that no Nigerian case law authority was found on Section 370 of the Criminal Code. Cf below Para 6.2.3.

- (b) trespass to land
- (c) trespass to property
- (d) nuisance
- (e) defamation
- (f) passing- off and
- (g) intentional infliction of emotional distress.

6.2.1.1 Breach of Confidence

Since English Common Law and rules of equity are applicable in Nigeria by virtue of the received law,¹⁴⁹⁰ English law cases supporting the recognition of a right to privacy based on the principle of breach of confidence¹⁴⁹¹ will also be applicable in Nigeria. Thus it will be possible to bring an action for breach of confidence in Nigeria based on the English law breach of confidentiality principles.

On the basis of the English law of confidentiality,¹⁴⁹² a duty of confidence may also be imposed on persons engaged in certain professions with respect to information obtained professionally or in the course of their duty. For instance, doctors, lawyers, and bankers will be expected to maintain confidentiality with respect to information obtained in the course of business regarding their patients or clients. Certain professional codes of ethics

¹⁴⁹⁰ Cap 192 LFN 1990. Cf above Para 6.2.1.

¹⁴⁹¹ *Albert v Strange* [1849] 2 De G & Sm 652, 64 ER 293 (Ch); *Morison v Moat* [1851] 9 Hare 241.

¹⁴⁹² See the principles laid down in *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109. Cf above Para 3.2.2.1.1.

also require that professionals maintain confidentiality in their dealings with clients (or patients- as the case may be) in the course of their duty.¹⁴⁹³

It must be noted that no reported Nigerian case was found on breach of confidence.

6.2.1.1a Relevance to Internet Cafes

A parallel may be drawn between the nature of the work of the professionals listed above and Internet café personnel, who may come into contact with personal information regarding their clients in the course of their duty. In this regard, it is affirmed that a duty of confidentiality may also be imposed on Internet café personnel with regard to personal information obtained in the course of their duty.¹⁴⁹⁴

6.2.1.2 Trespass to Person

Trespass to the person comprises the following three torts: assault, battery and false imprisonment.¹⁴⁹⁵ Where an invasion of privacy involves the application of force to the plaintiff (battery), or putting the plaintiff in fear of imminent battery (assault), or,

¹⁴⁹³ For instance the Hippocratic Oath taken by doctors upon their induction which reads in part:

“What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself..”

Cf Ludwig Edelstein *The Hippocratic Oath: Text, Translation, and Interpretation* (1943) at 2.

¹⁴⁹⁴ Cf above Para 3.2.2.1.1a.

¹⁴⁹⁵ See Kodilinye op cit at 12.

unlawful physical restraining of the plaintiff's movement (false imprisonment), action may be brought based on trespass to the person.

6.2.1.2a Relevance to Internet Cafes

Where a person is threatened with violence in order to obtain information processed in an Internet café, an action for assault may be brought to protect his privacy. Similarly, where the plaintiff is beaten up, physically attacked, or where his/her movement is restrained in order to obtain information processed in an Internet café, the plaintiff may successfully bring action for the trespass.¹⁴⁹⁶

6.2.1.3 Trespass to Land

Trespass to land is committed where a person enters the land of another or places or projects any object upon such land unlawfully.¹⁴⁹⁷ Where a person commits trespass to the land of the plaintiff in invading his or her privacy, the plaintiff will have a cause of action for trespass to land. The courts have held that it is an actionable trespass to put one's hand through the window of the plaintiff's house, or to sit on the wall of the plaintiff's house.¹⁴⁹⁸

¹⁴⁹⁶ Cf above Para 3.2.2.1.2.1.

¹⁴⁹⁷ See Kodilinye op cit at 177.

¹⁴⁹⁸ *Dabira v Adelaja* (1973) 11 CCHCJ 97 at 100; Cf *S v Boshoff & Others* supra at 396.

The Nigerian courts have also held that a person is liable in trespass if, having entered the plaintiff's premises lawfully, he or she remains on the land after his right of entry has expired. Thus in *Balogun v Alakija*¹⁴⁹⁹ where the plaintiff initially allowed the defendant into his house, the defendant was held liable for remaining in the plaintiff's house after he had been ordered by the plaintiff to leave. It has been said¹⁵⁰⁰ that the action for trespass to land protects title to land i.e. ownership, or the rights of an occupant.

6.2.1.3a Relevance to Internet Cafes

Where a person unlawfully enters (for instance by breaking in) or remains unlawfully in an Internet café, to access personal information contained in the computers located on the Internet café's premises, an Internet café owner may successfully bring an action for trespass to protect his/her privacy.¹⁵⁰¹ In so doing, the Internet café owner may secure and ensure the privacy of other information contained in computers on the premises. It is doubtful whether a customer in an Internet café will qualify for protection under this tort since s/he is a mere licensee.

6.2.1.4 Trespass to Chattel/Property

¹⁴⁹⁹ [1963] 2 All NLR 175.

¹⁵⁰⁰ Cf Kodilinye op cit at 177ff.

¹⁵⁰¹ Cf South African cases of intrusions involving unlawful entry; above at Para 6.1.1.

Where a person unlawfully takes, receives or keeps goods or property belonging to another, there will be liability for trespass to property.¹⁵⁰²

6.2.1.4a Relevance to Internet Cafes

With regard to protection of information processed in Internet cafes, where an invasion of privacy involves the unlawful taking of software or other document or device (for example, floppy disk or flash disk) containing personal information relating to another, there will be liability for trespass to property in respect of such invasion under the Nigerian law of torts.

6.2.1.5 Nuisance

The tort of private nuisance is designed to protect the individual owner or occupier of land against substantial interference with his or her enjoyment of such land.¹⁵⁰³ In *Tebite v Nigeria Marine and Trading Co Ltd*,¹⁵⁰⁴ where loud and excessive noise and noxious fumes from the defendants' premises caused the plaintiff discomfort and inconvenience, the plaintiff was awarded damages for private nuisance "to assuage and appease him for his injured feelings and the discomfort he ... had to bear ... from the defendant."¹⁵⁰⁵

¹⁵⁰² See Kodilinye op cit at 17.

¹⁵⁰³ See Kodilinye op cit at 92.

¹⁵⁰⁴ Supra.

¹⁵⁰⁵ Ibid at 438

Similarly in *Abiola v Ijoma*,¹⁵⁰⁶ the plaintiff brought action for excessive noise and smell and was awarded damages and an injunction restraining further nuisance by the defendant.

Although interference with the plaintiff in these cases was caused by noise, fumes and smell, it is submitted that the principle of awarding damage for injured feelings and discomfort in respect of unwelcome interference,¹⁵⁰⁷ or intrusion, may, in essence, be extended to protect the right to privacy especially in cases involving the projection or placing of objects¹⁵⁰⁸ including electronic bugs and camera beams¹⁵⁰⁹ on to the land or premises of others in order to watch them.

It is further submitted that the principle of awarding damages for injured feelings and discomfort may be extended to cases where a person is constantly watched from off his or her premises, (for instance by a “peeping tom” or the media) with or without the use of technological devices. Such peeping constitutes interference with private life.¹⁵¹⁰

¹⁵⁰⁶ [1970] 2 All NLR 268 at 278.

¹⁵⁰⁷ See also Kodilinye op cit at 92ff, where he classifies private nuisance into three categories. The second category of private nuisance deals with “substantial interference with the plaintiff’s user and enjoyment of his land”

¹⁵⁰⁸ Cf *Jeffries v Duncombe* (1809) 11 East 227, where the defendant kept a lamp burning in front of the plaintiff’s house, the plaintiff’s action for nuisance succeeded.

¹⁵⁰⁹ *Tebite v Nigeria Marine & Trading Co Ltd* supra, *Abiola v Ijoma* supra, on the projection of objects on to the land of another. See also *Bankole v Admekwe* (1973) 12 CCHCJ 97.

¹⁵¹⁰ Cf Corbett JA in *S v Naude* 1975 (1) SA 681 (A) at 704 A-B: where he observed, that the exercise of certain powers (the inquisitorial power of a commission of inquiry) interfered with the right of the

6.2.1.5a Relevance to Internet Cafes

The utility of this tort for the protection of privacy in Internet cafes is indeed limited as action can only be successfully brought by the Internet café owner. It is doubtful whether Internet cafe staff will qualify as occupants. However, the tort of nuisance may be relevant for the protection of privacy in Internet cafes where, for instance, a third party installs a spying device in order to gather information concerning customers on Internet café premises. In such a case, the Internet café owner may bring action in nuisance in respect of the invasion of privacy.

6.2.1.6 Defamation

The tort of defamation protects against injury to reputation resulting from words written or spoken by and to others.¹⁵¹¹ This tort affords protection for the right to privacy particularly with regard to the publication of private facts. Where the defendant said that the plaintiff, a tenant, had “brought strange people into the house day and night, smoking nauseating substances”, the court held the defendant liable for defamation.¹⁵¹²

The courts have also held that there is liability for defamation where a person said that a stevedoring and general contractor lived a life of wanton gluttony and immorality.¹⁵¹³

individual to the “tranquil enjoyment of his peace of mind.” See also *McQuoid-Mason* in *Chaskalson et al* op cit at 18-4.

¹⁵¹¹ Cf above Para 3.2.2.1.2.3. See *Kodilinye* op cit at 131ff.

¹⁵¹² *Mutual Aid Society Ltd. V Akerele* [1966] NMLR 257, see also *Karunwi v Wema Bank Ltd.* [1977] 3 CCHCJ 61 (affirmed (1975) 1 SC 15).

¹⁵¹³ *Bakare v Oluwide* [1969] 2 All NLR 324.

6.2.1.6a Relevance to Internet Cafes

Where a person publishes defamatory information or comments about another via e-mail or on the Internet, such publication will be actionable and (privacy) protection will be available to the plaintiff under the tort of defamation.¹⁵¹⁴

6.2.1.7 Passing-Off

The tort of passing-off protects the goodwill and reputation of the plaintiff's business or trade.¹⁵¹⁵ In this regard, Nigerian courts have held that there is passing-off in the following circumstances: where the defendant trades under a name so closely resembling that of the plaintiff as to be likely to mislead the public that the defendant's business and that of the plaintiff are the same;¹⁵¹⁶ and, where the defendant imitates the appearance or get up of the plaintiff's goods.¹⁵¹⁷ There will also be liability for passing off where the defendant markets his goods as those of the plaintiff.¹⁵¹⁸

¹⁵¹⁴ Cf the English case of *Godfrey v Demon Internet Ltd* supra.

¹⁵¹⁵ Kodilinye op cit at 215. Cf above Para 3.2.2.1.2.5

¹⁵¹⁶ *Hendriks v Montagu* (1881) 50 LJ Ch 456; *Niger Chemists Ltd v Nigeria Chemists* [1961] All NLR 171; *Ogunlende v Babayemi*(1971) 1 UILR 417.

¹⁵¹⁷ *U.K. Tobacco Co Ltd v Carreras Ltd* (1931) 16 NLR 1; *De Facto Works Ltd v Odumotun Trading Co Ltd* [1959] LLR 33.

¹⁵¹⁸ Cf Kodilinye op cit at 215.

The interest of privacy protected by the tort of passing-off falls under the category of appropriation. It protects the plaintiff from invasions of privacy by preventing wrongful attribution of authorship or publication.¹⁵¹⁹ It is often used for the protection of name or reputation in the business sector.

6.2.1.7a Relevance to Internet Cafes

The tort of passing-off will provide privacy protection in cases where business information is processed via the Internet and subsequently used unlawfully by another. Where for instance, an entrepreneur processes information in an Internet café regarding his or her idea for a line of goods with a given name, if that information is retrieved by another from the memory of the Internet café computer and used by that other to market similar goods under a similar name in a manner that is likely to mislead the public into thinking that both businesses are the same, action will lie for passing off in respect of the business information unlawfully obtained and used.

6.2.1.8 Intentional Infliction of Emotional Distress

This tort has been classified as an action relating to the tort of deceit and negligent misrepresentation.¹⁵²⁰ In this regard, the principle in *Wilkinson v Downton*¹⁵²¹ has been expounded thus: where a person makes a false statement which results in another

¹⁵¹⁹ Cf *Lord Byron v Johnston* Supra.

¹⁵²⁰ Kodilinye op cit at 292 – 293.

suffering nervous shock, there will be liability for the deceitful statement.¹⁵²² An examination of the United Kingdom authorities¹⁵²³ decided on the principle of *Wilkinson v Downton* however seems to suggest that the essential factor for an action under this head to succeed is that the plaintiff's peace of mind or mental health be disturbed by the defendant's action. In this regard, it does not appear to be significant whether the statement that resulted in the plaintiff's nervous shock is true or false.¹⁵²⁴

On the contrary, for an action based on the tort of deceit to succeed, it must be proved that the defendant knew the representation to be false, or, had no genuine belief in its truth.¹⁵²⁵ It is therefore respectfully submitted that to classify the principle laid down in *Wilkinson v Downton* as tort of deceit would deviate from the principle as originally laid down, and limit the application of the tort.¹⁵²⁶

6.2.1.8a Relevance to Internet Cafes

For our purposes, it is submitted that there will be liability for invasion of privacy under this tort, where a person suffers emotional distress as a result of an Internet café owner or

¹⁵²¹ Supra. Cf above Para 3.2.2.1.2.6.

¹⁵²² Kodilinye op cit at 292 – 293.

¹⁵²³ *Burnett v George* supra. See also *Janvier v Sweeney* supra.

¹⁵²⁴ See Lunney & Oliphant op cit at 54,55. According to them, this tort is available in respect of “intentional acts the inevitable consequence of which is physical (or psychological) harm” at 54. Cf W V H Rogers (ed.) *Winfield & Jolowicz on Tort* (1994) at 17,74.

¹⁵²⁵ Cf Kodilinye op cit at 208, 213 –214.

other personnel making a statement, or disclosing information based on information accessed in an Internet café, for instance, from another's e-mail.

6.2. 2 Common Law Protection of Data in Nigeria

As was the case under English Common Law prior to the adoption of the Human Rights Act,¹⁵²⁷ only limited protection can be found in Nigeria for data protection, in cases where the misuse of information involves the commission of a tort. In this regard, the equitable action for breach of confidence, as well as the torts of trespass, defamation, and, possibly, nuisance, passing –off and intentional infliction of emotional distress would be relevant for the Common Law protection of data.

6.2.2.1 Breach of Confidence

Where personal information or data is disclosed by the plaintiff to a person with regard to whom a duty of confidence may be implied, if that information is subsequently published or disclosed by that other, the plaintiff will be able to bring action for the disclosure under the principle of breach of confidentiality.

6.2.2.1a Relevance to Internet Cafes

¹⁵²⁶ Cf *McLoughlin v O'Brian* supra; *Vernon v Bosley* supra. See generally Lunney & Oliphant op cit at 56, 275ff.

¹⁵²⁷ 1998 Chapter 42 (Section 8). See above Chapter 3.

As observed above,¹⁵²⁸ the duty of confidentiality that exists between patients/clients/customers and professionals in the medical, legal and banking sectors based on the fact that they come into contact with personal/ sensitive information may be considered applicable to Internet café personnel, who also come into contact with personal information or data regarding their clients in the course of their duty.¹⁵²⁹ Thus, Internet café personnel will be liable for breach of a duty of confidence in respect of any unlawful disclosure of data processed in Internet cafes.

6.2.2.2 Trespass to Land

Where information is unlawfully obtained by means of an unlawful entry, action may be brought in respect of the unlawful entry where the defendant can show either ownership or lawful possession of the land.

6.2.2.2a Relevance to Internet Cafes

As previously mentioned,¹⁵³⁰ customers in Internet cafes have neither ownership nor possession rights but are mere licensees therefore it is doubtful whether a customer in an Internet café will qualify for protection under this tort. However, an Internet café owner may bring an action for trespass in respect of unlawful entry on Internet café premises

¹⁵²⁸ Cf above Para 6.2.1.1a.

¹⁵²⁹ See also above Para 3.2.2.1.1a.

¹⁵³⁰ Cf above Para 6.2.1.3a.

and or access to data contained in the computers located on the premises and may, by so doing, secure the privacy of the persons to whom the data contained in the computers relate.¹⁵³¹

6.2.2.3 Trespass to Property

Until the late 1990s, in Nigeria, very few individuals or businesses had access to computers. Most of the information processed in Nigeria, was stored in paper form. In this regard, it would have been possible to maintain an action based on the tort of trespass where information contained on paper was unlawfully taken or/and used. Nonetheless, action will lie for the unlawful taking of diskettes, flash drives and other portable devices in which information may be stored today.

6.2.2.2a Relevance to Internet Cafes

The tort of trespass to property will provide protection in respect of data infringement where any recording or copying device (for example, floppy disk or flash disk) or other computer software or document containing data relating to another is unlawfully taken or accessed.¹⁵³²

6.2.2.4 Nuisance

¹⁵³¹ Cf South African cases of intrusions involving unlawful entry; above at Para 6.1.1.

¹⁵³² Cf above Para 6.2.1.4a.

Where the obtaining of information regarding another involves interference with the peaceful enjoyment with their property action will lie for nuisance. Thus where, for instance, surveillance cameras are unlawfully installed for information- gathering, the tort of nuisance may provide a remedy for such unlawful gathering of information.

6.2.2.4a Relevance to Internet Cafes

As observed above,¹⁵³³ customers in Internet cafes will not be able to benefit from this tort, nor does it appear that Internet café employees can successfully bring action for nuisance.¹⁵³⁴ However, where, for instance, a third party installs a spying or recording device in order to gather data relating to customers on Internet café premises, an Internet café owner may bring action for nuisance in respect of the invasion of privacy.

6.2.2.5 Defamation

Where the disclosure or publication of personal information causes injury to the reputation of the plaintiff, there will be tortious liability for defamation in respect of such disclosure/publication.

6.2.2.5a Relevance to Internet Cafes

¹⁵³³ Cf above Paras 6.2.1.5 & 6.2.1.5a.

¹⁵³⁴ Ibid.

Where the disclosure or publication of data obtained via an Internet café results in injury to the reputation of the person to whom the data relates, there will be liability for defamation in respect of such disclosure or publication.¹⁵³⁵ There will also be liability for unlawful disclosure or publication of data effected by means of computers in an Internet café where the material published is defamatory. Thus the publication of information or data amounting to defamation via e-mail processed through computers in Internet cafes will be actionable and protection will be available to the plaintiff under the tort of defamation.¹⁵³⁶

6.2.2.6 Passing-Off

Where the misuse of business information involves the imitation of the appearance or get up of the plaintiff's name or business idea such that the public is misled into thinking that the plaintiff or his/her business is the same as the defendant's, there will be liability for passing off in respect of the unlawful use of information.

6.2.2.6a Relevance to Internet Cafes

Since the tort of passing-off primarily protects business interest, its utility for the protection of data in Internet cafes will be limited as it may safely be presumed that the

¹⁵³⁵ Cf above Para 6.2.1.6a.

¹⁵³⁶ Cf the English case of *Godfrey v Demon Internet Ltd* supra.

processing of sensitive business information or data will be uncommon, knowing the semi-public nature of Internet cafes. However, where, for instance, the name, market research statistics or ideas amounting to data, generated by a business is processed in an Internet café and is subsequently is retrieved and used by another in a manner that is likely to mislead the public into thinking that the businesses of the plaintiff and the defendant are the same, action will lie for passing off in respect of the business information unlawfully obtained and used.

6.2.2.7 Intentional Infliction of Emotional Distress

Where the plaintiff's peace of mind or mental health is disturbed as a result of the defendant's statement, the defendant will be liable for the infliction of emotional distress in respect of the information so-disclosed.

6.2.2.7a Relevance to Internet Cafes

Where a person suffers emotional distress as a result of an Internet café owner, staff or a third party making a statement, sending e-mail or otherwise disclosing or using personal information or data, accessed from a computer in an Internet café to make a statement, there will be liability for intentional infliction of emotional distress in respect of the data disclosure or use.

6.2.3 Conclusion on Common Law Protection of Privacy and Data in Nigeria

From the above, it is clear that there is very little Common Law protection available in Nigeria for privacy and data. Although Nigerian privacy law derives from the English Common Law, which is limited in the failure to recognise a right to privacy, the shortcomings of the Nigerian Common Law are different from that of the United Kingdom. In fact, it appears that the Nigerian courts have not maximised the positive features in the English Common Law. For instance, in the United States of America, the Common Law right to privacy was developed using the early Victorian English cases.¹⁵³⁷

In this regard, it is submitted that certain decisions of the English Common Law courts,¹⁵³⁸ if followed by Nigerian courts, would have resulted in better development of Nigerian privacy laws.¹⁵³⁹ Furthermore, since the Nigerian courts are free to develop the Common Law - in this case, the right to privacy and data protection, they are not bound by any imperfections in the English Common Law.¹⁵⁴⁰

In line with the above, it may be safely argued that the lack of creativeness of the Nigerian courts is a major contributory factor to the poor development of the Nigerian Common law generally, and the right to privacy specifically. However, the paucity of Nigerian cases is also highly significant. Since the courts can only develop the law in

¹⁵³⁷ Cf Warren & Brandeis "The Right to Privacy" (1890) 4 *Harvard Law Review* 193 at 207-212.

¹⁵³⁸ For example, *Albert v Strange* supra; *Morison v Moat* supra; *X v Morgan Grampian Publishers Ltd* supra, where the Appeal Court suggested that a thief who steals a document which is obviously confidential may be impressed with a duty of confidence. Cf above Para 3.2.2.1.1.

¹⁵³⁹ Cf the German Civil Courts' construction of the Civil Code above Para 5.2.

response to cases brought before them, there is a correlative need for actions to be brought before the courts if they are to fulfil their duty of legal development. The cause of the dearth of Nigerian privacy and data invasion cases must thus be found and solutions to the problem sought.

Possible suggestions for causative factors include Nigeria's slow technological development,¹⁵⁴¹ its socio-political history,¹⁵⁴² culture¹⁵⁴³ and, very significantly, poverty. In sum, Common Law protection of privacy and data in Nigeria is almost non-existent. There is ample room for growth and development to achieve a better standard of privacy and data protection in the Nigerian Common law. However, there is a corresponding need for change by the judiciary and the people in order to maximise the potential for privacy and data protection inherent in the Nigerian Common Law.

6.2.3a Relevance to Internet Cafes

¹⁵⁴⁰ Cf above Para 6.2.1.

¹⁵⁴¹ Until 1990, most record-keeping in Nigeria was largely paper-based and computer transactions were few and far between. Cf above Para 6.2.2.3. Today however, Internet services, electronic mail, telephone and facsimile are much more accessible, and may be regarded as basic office equipment. The availability of these technological devices has heightened general awareness about privacy issues.

¹⁵⁴² Cf above Para 1.5.

¹⁵⁴³ To illustrate this, Section 370 of the Nigerian Criminal Code (Northern Region) (now Cap 77 LFN1990) makes it an offence for a person to marry while his or her husband or wife is still alive, and while the (first) marriage is still valid. However, marriage to more than one wife, although no longer common, is not only accepted in Nigeria in the various cultures, but it is also recognised as valid and binding under customary law, as well as Islamic law. It was therefore not unusual for a man, having been married (in a court or church) under the Marriage Act, to marry another wife under customary law. This was the situation in *The Queen v Bartholomew Princewell* (1963) 2 All NLR 31 and the accused was found guilty of bigamy. He was sentenced to one month's imprisonment even though the law prescribes a maximum penalty of seven years for bigamy. Reed J, (the trial judge) observed (at 31) that he had not been referred to, and was unable to find any reported case on that section of the Criminal Code.

The observations above apply to the protection of privacy and data in Internet cafes. However, it is submitted that the failure to develop Common Law principles regarding the protection of privacy and data will have more far-reaching effects for Internet cafes as a restrictive approach to the interpretation of available laws is likely to result in the denial of protection in novel cases. Many Internet related cases of privacy and data invasions will fall into the category of new cases.

It will therefore be re-iterated in conclusion that the Nigerian Common Law is developable. However, the courts need to adopt a similar approach to that of the German Courts¹⁵⁴⁴ and solutions must be found to problems surrounding the extremely low litigation rate in order to achieve better privacy and data protection under the present Common Law principles.

6.3 Conclusion on Common Law Protection of Privacy and Data in South Africa and Nigeria

The analysis of the protection afforded privacy in South Africa and Nigeria and the development of the law in these two countries emphasises the difference between Civil Law and Common Law privacy protection. The recognition of personality rights under South African Common Law provides a firm foundation for the courts on which to build the right to protection of privacy, while the dependence on nominate torts under the Common Law restricted the available protection and constrained legal development.

¹⁵⁴⁴ Cf above Para 5.2.

Thus while there is adequate provision for the protection of privacy under South African Common Law, under which invasions of privacy in Internet cafes may be conveniently fit, in Nigeria, the Common Law has not been sufficiently developed to accommodate privacy and data invasions especially with regard to Internet cafes. In this regard, as asserted above, reliance on the breach of confidence cases might have been more productive.¹⁵⁴⁵ The Nigerian Constitution also provides room for development of the right to privacy and protection of data.¹⁵⁴⁶ Suggestions for this will be offered below.¹⁵⁴⁷

As for data, the South African Common Law provides protection in certain cases of data infringement, some of which is applicable to Internet cafes. However, the advancement of technology has made the protection of data a more complex issue requiring specific and comprehensive laws in order to achieve effective protection. Thus, South African Common Law data protection, though available, is at present inadequate to satisfy present day data protection needs.

In Nigeria however, the poor development of the Common Law bears on its data protection provisions. There are no general principles providing for the misuse of information and claims are restricted to the torts. Nigerian Common Law therefore affords little or no data protection. Clearly, there is a contrast between South African

¹⁵⁴⁵ *Albert v Strange* supra; *Morison v Moat* supra.

¹⁵⁴⁶ *Ibid.*

¹⁵⁴⁷ Chapter 6.

Common Law protection, which is available even though limited, and Nigerian Common Law data protection, which is virtually undeveloped and unavailable.

In sum, it may be concluded from the above that although the South African Common Law has hitherto been effective in protecting the right to privacy, it is limited in the protection of data. As for Nigeria, it is submitted that at present, the Common Law does not protect adequate provision for privacy or data, either generally or with regard to information processed in Internet cafes. There is an unequivocal need to develop the Common Law regarding privacy. There is also an immense gap in the area of data protection, which will need to be filled with detailed data protection legislation.

We shall now proceed to examine the constitutional provisions and available statute law on privacy and data protection in South Africa and Nigeria.

CHAPTER SEVEN

CONSTITUTIONAL AND STATUTE LAW PROTECTION OF PRIVACY AND DATA IN SOUTH AFRICA AND NIGERIA

7.1 Statutory Protection of Privacy and Data in South Africa

7.1.1 Constitutional Protection

7.1.1.1 Constitutional Protection of Privacy in South Africa

Section 14 of the South African Constitution¹⁵⁴⁸ provides that:

“Everyone has the right to privacy, which includes the right not to have-

- (a) their person or home or property searched;
- (b) their property searched;
- (c) their possessions seized; or
- (d) the privacy of their communications infringed.”

This section provides for a general right to privacy as well as the four categories of privacy rights specified.¹⁵⁴⁹ By specifying these four categories, this section sets out

¹⁵⁴⁸ Act 108 of 1996.

specific aspects of the right included in the provision. It has however been said with regard to the general right to privacy provided for, that it extends to any other method of obtaining information or making unauthorised disclosure.¹⁵⁵⁰ Accordingly, in *Klein v Attorney-General WLD & Another*,¹⁵⁵¹ the unlawful restoration of information erased by its owner and given to the state for use in a criminal prosecution was held to be a violation of the applicant's right to privacy under Section 13 of the Interim Constitution.

In the construction of the constitutional guarantee of privacy, it has been said that the constitutional right to privacy should be given a benevolent interpretation, and should also be read with similar rights protected in other sections of the Constitution, (such as the right to human dignity guaranteed in section 10).¹⁵⁵² It has also been suggested in this regard that the right to personal privacy should be interpreted as guaranteeing to each citizen an inviolable sphere of privacy beyond the reach of public authority.¹⁵⁵³

¹⁵⁴⁹ Cf D McQuoid-Mason "Privacy" in M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz, S Woolman *Constitutional Law of South Africa* (1996) at 38-19. See also J De Waal, I Currie & G Erasmus *The Bill of Rights Handbook* (2000) at 372.

¹⁵⁵⁰ Cf McQuoid-Mason in "Privacy" op cit at 38-11.

¹⁵⁵¹ 1995 (3) SA 848 (W) at 865.

¹⁵⁵² L du Plessis & J de Ville "Personal Rights" in D van Wyk, J Dugard, B de Villiers & D Davis (eds) *Rights and Constitutionalism* (1994) at 252.

¹⁵⁵³ *Ibid.*

The test for a constitutional invasion of privacy is, as in the United States ¹⁵⁵⁴ that the plaintiff has a reasonable expectation of privacy.¹⁵⁵⁵ In essence, when there has been an infringement of the constitutional right to privacy, the courts must determine whether the plaintiff had a reasonable expectation of privacy in the circumstances.¹⁵⁵⁶ The Constitutional rights to privacy provided for have been generally classified as privacy rights protecting personal autonomy (substantive privacy rights),¹⁵⁵⁷ on the one hand, and privacy rights protecting information (informational privacy rights)¹⁵⁵⁸ on the other hand.¹⁵⁵⁹

Substantive privacy rights protect the individual against intrusions and other interferences with private life, while informational privacy rights deal with access to, disclosure and other use of information.¹⁵⁶⁰ Where, for instance, there is unlawful disclosure of information obtained from a personal computer, which has been wrongfully seized in the course of an unlawful search of an individual's home, this would amount to an invasion of the constitutional right provided for in section 14(a). The unlawful search and seizure of property will be an infringement of substantive privacy rights, while the misuse of

¹⁵⁵⁴ See Ackermann J in *Bernstein v Bester* supra at Para 75.

¹⁵⁵⁵ Ibid. Cf also *National Coalition for Gay & Lesbian Equality & Others v Minister of Justice & Others* 1998 (6) BCLR 726 (W); 2 SACR 102 (W).

¹⁵⁵⁶ Cf *S v Zwayi* 1998 (2) BCLR (CK) where it was affirmed that the expectation of privacy must be reasonable in the circumstances and refusal to provide identification to a police officer when so requested will not qualify.

¹⁵⁵⁷ Cf above Para.3.2.1a.

¹⁵⁵⁸ Cf above Para3.2.1b.

¹⁵⁵⁹ See McQuoid-Mason op cit in Chaskalson et al op cit at 18-8.

information retrieved from the seized computer will constitute a violation of informational privacy rights.

With regard to substantive privacy rights, the courts in South Africa have upheld the right to privacy with regard to (pornographic photographic) materials kept within the home.¹⁵⁶¹ The courts have also upheld the right to decide who may enter one's home in the context of unlawful searches and seizures.¹⁵⁶² As for informational privacy rights, generally, any unlawful use of information, which violates a person's right to privacy will be actionable. In this regard, the restoration of information on a computer system has been held to violate the plaintiff's right to privacy.¹⁵⁶³

The constitutional guarantee of the right to privacy also protects the right of an individual not to disclose information.¹⁵⁶⁴ Neethling's¹⁵⁶⁵ definition of privacy is particularly relevant here. According to him, privacy is "an individual condition of life characterised by exclusion from publicity." In his view, "This condition includes all those personal facts which the person himself [or herself] at the relevant time determines to be excluded

¹⁵⁶⁰ Cf above Para 3.2.1.

¹⁵⁶¹ *Case & Another v Minister of Safety and Security & Others* 1996 (3) SA 617 (CC), 1996 (5) BCLR 609 (CC). See Didcott J at Para 91.

¹⁵⁶² *State v Gumede & Another* 1998 (5) BCLR 530 (D); *S v Madiba & Another* 1998 (1) BCLR 38 (D) at 43. Cf *McQuoid-Mason* in *Chaskalson et al op cit* at 18-9.

¹⁵⁶³ *Klein v Attorney General, WLD, & Another supra*. Cf above Para 5.1.1.1.

¹⁵⁶⁴ *Bernstein v Bester supra*. See Ackermann J at Para 58.

¹⁵⁶⁵ J Neethling, J M Potgieter, P J Visser *Law of Delict* (2006) 5th ed at 355; Neethling *Persoonlikheidsreg* (1985) 39-40

from the knowledge of outsiders and in respect of which he [or she] evidences a will for privacy.”¹⁵⁶⁶ Hence it may be said that the essence of the individual’s interest in his/her privacy is the power to determine for him/herself the scope of his/her interest in privacy.¹⁵⁶⁷ Neethling’s definition has been accepted by the South African Supreme Court of Appeal¹⁵⁶⁸ in *National Media Ltd v Jooste*¹⁵⁶⁹ where the court upheld “informational privacy” rights.¹⁵⁷⁰

Where information is reasonably required by the State pursuant to a statute¹⁵⁷¹ collection of information will be deemed “reasonable and justifiable” and so will not constitute an invasion of privacy under section 14.¹⁵⁷² It has been established however that, where the answer to any question will infringe on or threaten an examinee’s rights guaranteed under the Constitution, such question will be regarded as having been unlawfully put.¹⁵⁷³

¹⁵⁶⁶ 1996 (3) SA 262 (A) at 271.

¹⁵⁶⁷ Cf Roos op cit at 556ff.

¹⁵⁶⁸ (Formerly South African Appellate Division) See also *Jooste v National Media Ltd* 1994 (2) SA 634 (C) at 645, *Bernstein v Bester NO* 1996 2 SA 751 (CC) at 789.

¹⁵⁶⁹ 1996 (3) SA 262 (A) at 271.

¹⁵⁷⁰ See also *Jooste v National Media Ltd* 1994 (2) SA 634 (C) at 645, *Bernstein v Bester NO* 1996 2 SA 751 (CC) at 789.

¹⁵⁷¹ For instance the Statistics Act (Act 66 of 1976), which requires the furnishing of information (section 16); and the Criminal Procedure Act (Act 51 of 1977) which requires the answering of questions (section 205); Cf below chapter 5.

¹⁵⁷² See McQuoid-Mason in Chaskalson et al op cit at 18-12. Cf J Neethling *Law of Personality* (2005) at 294.

¹⁵⁷³ *Bernstein v Bester* supra at Para 61. See also *Nel v Le Roux No & Others* 1996 (3) SA 562 (CC), 1996 (4) BCLR 592 (CC) at Para 18.

The courts must also recognise and apply common law principles where they are not in conflict with any constitutional provisions or constitutional values.¹⁵⁷⁴ In essence, the common law and the constitutional provisions protecting privacy must be read together to protect privacy,¹⁵⁷⁵ and the constitutional guarantee of privacy will be instrumental in developing the common law action for invasion of privacy.¹⁵⁷⁶ In this regard, newly created substantive and informational privacy rights, some of which confer personal interests on individuals as against the State have been identified.¹⁵⁷⁷

It must be noted that the rights guaranteed by the Constitution are limited in terms of Section 36 of the Constitution, which provides that:

“[T]he rights in the Bill of Rights may be limited ... to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors including (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose.”

¹⁵⁷⁴ *Gardener v Whitaker* 1995 (2) SA 672 (E) at 684. Cf *McQuoid-Mason in Chaskalson et al op cit* at 18-2.

¹⁵⁷⁵ Cf *D McQuoid-Mason “Invasion of Privacy: Common Law v Constitutional Delict- Does it make a Difference?”* (2000) *Acta Juridica* 227 at 260 –261.

¹⁵⁷⁶ *McQuoid-Mason in Chaskalson et al op cit* at 18-8.

¹⁵⁷⁷ *Ibid.* Cf American cases on substantive and informational privacy rights. See generally above Para 4.1.1.

In effect, where an administrative action or the provisions of any legislation would be, or cause, an infringement of the right to privacy or interfere with the protection guaranteed by the right to privacy, such act or legislation would be justified if the infringement falls within the requirement of section 36.¹⁵⁷⁸ For instance, the Criminal Procedure Act¹⁵⁷⁹ also provides for the search of persons, under certain circumstances, even though searches and seizures generally involve a violation of a person's right to privacy.¹⁵⁸⁰ Such searches, which are permitted in the interests of justice, must comply with the provisions of the Act in order to remain lawful.¹⁵⁸¹

The Interception and Monitoring Prohibition Act¹⁵⁸² prohibits the interception of telecommunications or monitoring of communications with the use of monitoring devices unless authorised by a judge on specific grounds. In *S v Naidoo*,¹⁵⁸³ it was asserted that the Interception Act complies with the requirements of Section 36 of the Constitution.

In *Case & Another v Minister of State and Security & Others*,¹⁵⁸⁴ the Constitutional Court ruled that section (2) 1 of the repealed Indecent or Obscene Photographic matter

¹⁵⁷⁸ See also du Plessis & de Ville in van Wyk et al op cit at 253.

¹⁵⁷⁹ Act 51 of 1997.

¹⁵⁸⁰ See *Fedics v Matus* 1997 (BCLR) 1199 (C) at Para 97. Cf *McQuoid-Mason* in Chaskalson et al op cit at 18-13 – 18-14.

¹⁵⁸¹ *S v Motloutsi* 1996 (1) SA 584 (C), at 592-593, 1996 (2) BCLR 220 (C), See also *S v Human & another* 1996 (1) SA 232 (W) at 233, 237. Cf *Mistry v Interim National Medical and Dental Council of South Africa & others* 1998 (7) BCLR 880 (CC) where the Court held that the invasion authorised by section 28(1) of the Medicines and Related Substances Control Act (101 of 1965) was disproportionate to its public purpose. (Per Sachs J at Para 27).

¹⁵⁸² 127 of 1992.

¹⁵⁸³ [1998] 1 All SA 189 (D) 213.

¹⁵⁸⁴ 1996 (3) SA 617 (CC), 1996 (5) BCLR 609 (CC).

Act,¹⁵⁸⁵ which prohibited the possession of “indecent or obscene photographic matter” was an unconstitutional limitation of the right to privacy.” The court held that the right to privacy included the right to possess obscene matter in the seclusion of one’s home.

However, in *Bernstein v Bester*,¹⁵⁸⁶ the Constitutional Court held that the provisions of sections 417 (3) and 418 (2) of the Companies Act which compel the production of private documents were justifiable in terms of Section 33(1) of the Interim Constitution,¹⁵⁸⁷ even though such production of documentation constituted a ‘seizure’ within the meaning of Section 13 of the Interim Constitution.¹⁵⁸⁸ In *Bernstein*’s case, the court weighed the interest of the creditors and the community against the alleged infringement of the right to privacy.¹⁵⁸⁹

From the above, it will be seen that both the Constitution and common law provide for the protection of the right to privacy and limit the scope of the protection provided for, in terms of the defences available for infringements of privacy under their provisions. However, the requirements for establishing an infringement of privacy at common law

¹⁵⁸⁵ Act 37 of 1967.

¹⁵⁸⁶ 1996 (2) SA 751 (CC), 1996 (4) BCLR 449 (CC).

¹⁵⁸⁷ Act 200 of 1993; Section 33(1), like Section 36 of the 1996 Constitution, provided for limitation of rights under the Constitution.

¹⁵⁸⁸ Section 13 of the Interim Constitution, like section 14 of the 1996 Constitution, guaranteed a right to personal privacy including the right not to be subject to searches, seizure of private possessions or the violation of private communications.

¹⁵⁸⁹ At Para 90.

are different from those necessary for establishing a constitutional infringement of privacy.¹⁵⁹⁰

At common law, the unlawfulness, or wrongfulness of the act is one of the key elements to be determined by the courts,¹⁵⁹¹ and if the defendant provides a lawful justification or relies on a defence negating unlawfulness,¹⁵⁹² there will be no liability. Under the Constitution on the other hand, once there has been an infringement of the right to privacy as set out in the Constitution, and the plaintiff has been shown to have a reasonable expectation of privacy,¹⁵⁹³ a defendant cannot rely on the defences negating unlawfulness but on section 36 of the Constitution.¹⁵⁹⁴ The questions to be asked in this regard, are:

- (1) whether the plaintiff had a reasonable expectation of privacy and
- (2) whether the infringement is justifiable¹⁵⁹⁵

It has been established that there is no closed list of possible exemptions permissible by virtue of section 36.¹⁵⁹⁶

¹⁵⁹⁰ See Ackermann J in *Bernstein v Bester* supra at Para 71.

¹⁵⁹¹ Ibid. See also J Neethling, J M Potgieter, P J Visser *Law of Delict* (1999) at 355. Cf above Para 4.1.1.1.

¹⁵⁹² Cf Neethling et al op cit at 355. Cf above Para 4.1.1.4.

¹⁵⁹³ Cf McQuoid-Mason (2000) *Acta Juridica* 227 at 247. Cf Ackermann J in *Bernstein v Bester* op cit at Para 75.

¹⁵⁹⁴ See McQuoid-Mason (2000) *Acta Juridica* 227 at 246.

¹⁵⁹⁵ Ibid.

Finally, juristic persons are also afforded protection under the Constitution. Section 8 (2) provides that:

“A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right”

Section 8 (3) (a) requires the courts to develop the Common Law in order to give effect to a provision of the Bill of Rights, when relying on S 8 (2) of the Constitution. Accordingly, the courts have recognised that juristic persons can enjoy certain informational privacy rights.¹⁵⁹⁷

7.1.1.1a Relevance to Internet Cafes

To determine the practicality of its application for Internet café purposes, it is useful to determine whether the South African Constitution applies vertically as well as horizontally. In this regard, it has been affirmed¹⁵⁹⁸ that its application may be vertical¹⁵⁹⁹

¹⁵⁹⁶ *S v Manamela* 2000 (1) SACR 414 (CC) at 430.

¹⁵⁹⁷ *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd & Another* 1993 (2) SA 451 (A), *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A).

¹⁵⁹⁸ Neethling, Potgieter & Visser *Delict* op cit at 19-23. See also Roos op cit at 549.

¹⁵⁹⁹ Section 8(1) of the Constitution makes its provisions binding on the state and its organs.

as well as horizontal,¹⁶⁰⁰ and may be either direct¹⁶⁰¹ or indirect.¹⁶⁰² It is thus safe to affirm that the provisions contained in Section 14 of the South African Constitution as well as part d of Section 14, which specifically provides for the privacy of communications, will be relevant and applicable for our purpose. In effect, there will be protection against invasions of privacy in Internet cafes if a reasonable expectation of privacy can be shown to exist in the circumstances.

Thus, where anyone hacks into a computer or decodes a customer's password in order to access personal information relating to them, or, where a customer's e-mail is read by another, that customer will have a cause of action under the Constitution if he or she can prove a reasonable expectation of privacy in respect of the information accessed. The action will however succeed only if there is no justification for the acts amounting to the privacy invasion. There will also be liability under the Constitutional provisions for publication of personal information processed in an Internet café if the plaintiff can prove that s/he had a reasonable expectation of privacy and if there is no justification for such infringement.

7.1.1.2 Constitutional Protection of Data in South Africa

¹⁶⁰⁰ Section 8(2) makes the Constitutional provisions binding on natural and juristic persons

¹⁶⁰¹ See Section 8(3). The direct operation of the Constitution means the courts must apply and where necessary, develop the Common Law to give effect to the fundamental rights related to the law of delict to the extent to which legislation fails to do so.

¹⁶⁰² Section 39(2). This means that all private law principles and rules are subject to the basic values of the Constitution.

There is no specific legislation protecting data in the South African Constitution. However, the provisions guaranteeing privacy may also be construed for the protection of data.¹⁶⁰³ Thus where the collection, sorting, storage, retrieval, modification, disclosure or any other use of information amounts to an invasion of privacy as provided for in Section 14, there will be constitutional protection for such data infringement.

It must be mentioned that Section 32 of the Constitution of South Africa¹⁶⁰⁴ provides for access to information. It provides as follows:

“Everyone has the right of access to any information held by the state; and any information that is held by another person and that is required for the exercise or protection of any rights.”¹⁶⁰⁵

Section 32(2) further requires that the state enact national legislation to give effect to this right. Pursuant to this section, the Promotion of Access to Information Act¹⁶⁰⁶ has been enacted. The provision of Section 32 must however be balanced against the right to privacy in Section 14.

¹⁶⁰³ Cf *Klein v Attorney-General WLD & Another* supra where the unlawful restoration of information erased by its owner and given to the state for use in a criminal prosecution was considered. Cf R. Buys (ed) *Cyberlaw @ SA II: The Law of the Internet in South Africa* (2004) at 380. Cf McQuoid-Mason Chaskalson et al op cit at 38-11

¹⁶⁰⁴ Act 108 of 1996.

¹⁶⁰⁵ Section 32(1).

¹⁶⁰⁶ No 2 of 2000. Cf below Para 7.1.2.1.1.

7.1.1.2a Relevance to Internet Cafes

In line with the above, where the processing of data in Internet cafes amounts to an invasion of privacy in circumstances where the plaintiff can show that there was a reasonable expectation of privacy, provided that there is no justification for the act constituting the infringement, constitutional protection will be available. In addition, certain aspects of the Promotion of Access to Information Act¹⁶⁰⁷ will be relevant for the regulation of information processed in Internet cafes. The relevant portions of the Act will be discussed below.

7.1.2 Statutory Protection

7.1.2.1 Statutory Protection of Privacy in South Africa

There is no Privacy Act in South Africa but protection of aspects of privacy can be found in the following legislation: the Promotion of Access to Information Act,¹⁶⁰⁸ the Interception and Monitoring (Prohibition) Act,¹⁶⁰⁹ the Telecommunications Act,¹⁶¹⁰ the Telegraph Messages Protection Act,¹⁶¹¹ the Criminal Procedure Act,¹⁶¹² the Civil

¹⁶⁰⁷ No 2 of 2000. Cf below Para 7.1.2.1.1.

¹⁶⁰⁸ No 2 of 2000.

¹⁶⁰⁹ Act 127 of 1992.

¹⁶¹⁰ No 103 of 1996.

¹⁶¹¹ No 44 of 1963.

¹⁶¹² Act 51 of 1977.

Proceedings Evidence Act,¹⁶¹³ Natal Law to Amend the Law of Evidence,¹⁶¹⁴ the Copyright Act,¹⁶¹⁵ the National Credit Act¹⁶¹⁶ and the proposed Consumer Protection Act.¹⁶¹⁷ The relevant sections of these Acts will be discussed below.

7.1.2.1.1 The Promotion of Access to Information Act¹⁶¹⁸

The Promotion of Access to Information Act regulates access to information in South Africa pursuant to Section 32 (2) of the Constitution.¹⁶¹⁹ The Act allows for access to records kept by public¹⁶²⁰ and private bodies,¹⁶²¹ and also sets limitations on disclosure of such information. Part Two regulates access to records of public bodies while Part Three deals with records of private bodies.

The Preamble to the Act states that in giving effect to the constitutional right of access to information, the Act must have regard to and fulfil all the rights in the Bill of Rights and that the rights provided for by the Access to information Act may be limited in terms of

¹⁶¹³ No 25 of 1965.

¹⁶¹⁴ Evidence Law No 5, 1870.

¹⁶¹⁵ No 98 of 1978 .

¹⁶¹⁶ No 34 of 2005.

¹⁶¹⁷ 15 March 2006 (Gov Gazzette No 28629).

¹⁶¹⁸ No 2 of 2000.

¹⁶¹⁹ Constitution of the Republic of South Africa 1996.

¹⁶²⁰ Section 11.

¹⁶²¹ Section 50.

Section 36 of the Constitution. It further provides specifically in Section 9¹⁶²² that the Act aims to give effect to the Constitutional right of access to information, subject to justifiable limitations, including limitations aimed at the protection of privacy and commercial confidence.

The effect of Section 9 of the Act is that, in applying the provisions of the Act, generally regard will be had to the right to privacy, even where the provisions in question do not specifically provide for this.¹⁶²³ Apart from the general regard for privacy rights provided for, certain provisions of the Act that regulate disclosure and allow for the correction of incorrect records, also indirectly provide privacy protection.

The Act specifies the grounds on which access to records may be refused.¹⁶²⁴ These include mandatory protection of privacy of a third party who is a natural person;¹⁶²⁵ protection of commercial information of a third party;¹⁶²⁶ protection of the commercial information of a private body, (which includes trade secrets, financial, commercial, technical and scientific information, where the disclosure is likely to cause harm to financial or commercial interests);¹⁶²⁷ protection of certain records of the South African

¹⁶²² This section states the Objects of the Act.

¹⁶²³ Cf J Klaaren "Access to Information" in Chaskalson et al op cit at 248.

¹⁶²⁴ Part 2, chapter 4; part 3, chapter 4.

¹⁶²⁵ Section 34 & Section 63.

¹⁶²⁶ Section 36 & Section 64.

¹⁶²⁷ Section 68.

Revenue Service;¹⁶²⁸ information supplied in confidence;¹⁶²⁹ and protection of safety of the individual and of property.¹⁶³⁰

The Act also allows for rights of correction by persons affected by incorrect records¹⁶³¹ and protects certain official records and privileged information.¹⁶³² The Act specifically provides protection for health records.¹⁶³³ It states in respect of records provided by health practitioners about the physical or mental health or well being of a person, that access may only be given regarding such records after reasonably practicable steps have been taken to limit or alleviate possible harm to the physical or mental health or well-being of the person to whom the information relates upon disclosure.

7.1.2.1.1a Relevance to Internet Cafes

Although information is not deliberately recorded in Internet cafes and as such, they are not strictly data collection agencies, information gathering is incidental to their business as a result of the accumulation of information on their computer hard drives. Certain provisions of the Promotion of Access to Information Act may therefore be relevant for the regulation of access to or disclosure of such information.

¹⁶²⁸ Section 35.

¹⁶²⁹ Section 37 & Section 65.

¹⁶³⁰ Section 38 & Section 66.

¹⁶³¹ Section 88.

¹⁶³² Section 12, Section 41. See also *CCII Systems (Pty) Ltd v Fakie NNO* 2003 (2) SA 325 (T).

¹⁶³³ Section 30 & Section 61.

In this regard, Section 9 which makes consideration of the constitutional right to privacy relevant in determining whether to allow access to information will be instructive for Internet café cases. In effect, the constitutional guarantee of privacy should be considered in allowing or denying access to any information contained in Internet café depositories.

In addition, the provisions specifying the grounds for the refusal of access to records¹⁶³⁴ will be instructive for drawing similar limits with regard to access to information contained in Internet cafes. Thus, access to personal information contained in Internet café premises or equipment will be denied for the protection of: privacy of a third party who is a natural person;¹⁶³⁵ commercial information of a third party;¹⁶³⁶ commercial information of a private body,¹⁶³⁷ information supplied in confidence;¹⁶³⁸ safety of the individual and of property¹⁶³⁹ and the protection of health records.¹⁶⁴⁰

7.1.2.1.2 The Interception and Monitoring (Prohibition) Act¹⁶⁴¹

¹⁶³⁴ Part 2, chapter 4; part 3, chapter 4.

¹⁶³⁵ Section 34 & section 63.

¹⁶³⁶ Section 36 & section 64.

¹⁶³⁷ Section 68.

¹⁶³⁸ Section 37 & section 65.

¹⁶³⁹ Section 38 & section 66.

¹⁶⁴⁰ Section 30 & section 61.

¹⁶⁴¹ Act 127 of 1992.

The Interception and Monitoring (Prohibition) Act regulates the intentional interception and monitoring of certain communications¹⁶⁴² and its primary purpose is to protect confidential information from unlawful eavesdropping.¹⁶⁴³ It prohibits the interception or monitoring of telephone communications and other forms of telecommunication without the consent of at least one of the parties to the communication,¹⁶⁴⁴ or the authorisation of a judge.¹⁶⁴⁵ The Act also stipulates the conditions under which a judge may give authorization.¹⁶⁴⁶ Its provisions also apply to the interception of postal articles.¹⁶⁴⁷

Section 7 of the Act prohibits persons concerned with the performance of the functions of the Act from disclosing information acquired in the course of the performance of their functions under the Act, except in specified circumstances.¹⁶⁴⁸ The Act also has provisions on offences and penalties for non-compliance with its provisions.¹⁶⁴⁹ The 1992 Interception and Monitoring (Prohibition) Act will be replaced¹⁶⁵⁰ by the 2001 Interception and Monitoring Act¹⁶⁵¹ which incorporates the same principles contained in

¹⁶⁴² See generally the introductory paragraph, Sections 2, 6 & 7.

¹⁶⁴³ *S v Dube* 2000 (2) SA 583 (N); *Lenco Holdings Ltd & ors v Eckstein & ors* 1996 (2) SA 693 (N) at 700.

¹⁶⁴⁴ Section 2. See *S v Naidoo & anor* 1998 (1) BCLR 46 (N); See also *S v Dube* supra.

¹⁶⁴⁵ Section 3. See *S v Nkabinde* 1998 (8) BCLR 996 (N); *S v Naidoo & anor* supra.

¹⁶⁴⁶ Section 3.

¹⁶⁴⁷ Section 4.

¹⁶⁴⁸ Section 7(a-d).

¹⁶⁴⁹ Section 8.

¹⁶⁵⁰ Section 21 of the text of the 2001 Interception and Monitoring Bill 2001[B50-2001] provides for the repeal of the 1992 Act.

the 1992 Act, but widens its cope to cover Internet and cellular networks and communications.

It has been said¹⁶⁵² in respect of the 1992 Act, that the provisions specifying the conditions under which a judge may issue a direction for interception of communications or postal articles¹⁶⁵³ may be subject to scrutiny by the Constitutional Court to determine whether they are reasonable and justifiable, (in accordance with Section 36 of the Constitution). Furthermore, it has been affirmed¹⁶⁵⁴ that even if the conditions of Section 36 of the Constitution have been satisfied, where the provisions of the Act have not been properly followed, an action for invasion of privacy will lie under the Constitution.¹⁶⁵⁵

The Act does not have any specific provisions on participant monitoring. The courts have however held that there is no liability under the Act where information covering the criminal conduct of the communicator is voluntarily imparted by one of the parties in a two-party conversation.¹⁶⁵⁶ It was held in *S v Kidson*¹⁶⁵⁷ that the plaintiff's constitutional

¹⁶⁵¹ Section 22 of the Interception and Monitoring Bill provides: "This Act is called the Interception and Monitoring Act, 2001, and comes into operation on a date fixed by the President by proclamation in the Gazette".

¹⁶⁵² McQuoid-Mason in Chaskalson et al op cit at 18-6.

¹⁶⁵³ Section 3(1)(b), of the 1992 Act, Section 4(2)(a) & (b) of the 2001 Act.

¹⁶⁵⁴ McQuoid-Mason in Chaskalson et al op cit at 18-6.

¹⁶⁵⁵ Cf *S v Naidoo & Anor* 1998 (1) BCLR 46 (N); 1998 (1) SACR 478 (N) where the court observed that monitoring (of a conversation) not authorised by a direction properly and lawfully issued by a judge would constitute a violation of the Monitoring Act as well as an infringement of the Constitutional right to privacy (per McCall J at 72).

¹⁶⁵⁶ *S v Kidson* 1999 (1) SACR 338 (W).

¹⁶⁵⁷ *Ibid.*

right to privacy had not been breached where the monitoring was procured for the police by another, in a conversation with the accused.¹⁶⁵⁸ The court was of the opinion that the information imparted was not “confidential information” as provided for by the Interception and Monitoring Prohibition Act.¹⁶⁵⁹

Although the provisions of the Act clearly apply to individuals,¹⁶⁶⁰ by virtue of Section 1a of the Act, it appears that the Act only applies to state agencies to the exclusion of private agencies. In effect, there will be liability under the Act only for acts committed by individuals and state agencies. However, since interception and/or monitoring is often executed or aided by individuals (with the use of technological devices), it is submitted that, for the Interception Act to be maximally effective, and, in the absence of any provision specifically excluding private agencies from liability, it should be possible to pierce the veil of incorporation and hold the individuals who act on behalf of any private agency liable under the Act.

7.1.2.1.2a Relevance to Internet Cafes

This Act will be relevant where e-mail communication or a telephone communication that takes place in an Internet café is monitored or intercepted by an individual. Such monitoring or interception will be unlawful if not authorised or consented to by at least one of the parties to the communication. However, in the light of Section 1a of the Act it

¹⁶⁵⁸ Per Cameron J at 350 ff.

¹⁶⁵⁹ Per Cameron J at 348.

is doubtful as to whether there will be protection for communication intercepted in an Internet café, where interception is procured through a private agency.

7.1.2.1.3 The Telecommunications Act¹⁶⁶¹

This Act contains confidentiality provisions with regard to persons performing functions under the Act. It provides that:

“No councillor, member of a committee of council, expert appointed in terms of section 28, member of the staff of the authority or inspector appointed in terms of section 99, director or member of staff of the agency shall disclose any information in regard to any matter which may come to his or her knowledge in the performance of any function ... by virtue of the office held by him or her.¹⁶⁶²

7.1.2.1.3a Relevance to Internet Cafes

Although not directly relevant to Internet cafes, a similar provision rendering the disclosure by Internet café personnel of information pertaining to customers in Internet cafes unlawful would be useful for the protection of information processed in Internet cafes.

¹⁶⁶⁰ Section 2. See *S v Naidoo & anor* supra. Cf above.

¹⁶⁶¹ No 103 of 1996.

7.1.2.1.4 The Telegraph Messages Protection Act¹⁶⁶³

This Act prohibits the publication of telegraphic messages before a given time, except by the addressee, or with his or her consent.¹⁶⁶⁴

7.1.2.1.4a Relevance to Internet Cafes

This Act will not be of much relevance for the Internet café privacy protection since they do not process telegraph messages.

7.1.2.1.5 The Criminal Procedure Act¹⁶⁶⁵

Certain provisions of the Criminal Procedure Act confer privileges on certain classes of persons to refuse to disclose admissible evidence. Section 203 provides that a person shall not be compelled to answer questions that may expose him or her to a criminal charge. This provision protects the disclosural privacy of accused persons in criminal prosecutions with regard to potentially- incriminating information that they have in their possession about themselves.¹⁶⁶⁶

¹⁶⁶² Section 93.

¹⁶⁶³ No 44 of 1963.

¹⁶⁶⁴ Section 2.

¹⁶⁶⁵ Act 51 of 1977.

¹⁶⁶⁶ See *S v Kidson* supra.

The protection offered by this provision is analogous to the United States Constitutional guarantee of protection against self-incrimination contained in the 5th Amendment.¹⁶⁶⁷ It has also been said that the protection guaranteed by this provision in South Africa may apply to evidence that tends to disclose facts that might not be incriminating in themselves but that might “form links in the chain of proof against the witness.”¹⁶⁶⁸

Section 198 of the Criminal Procedure Act provides for the right of husbands and wives to refuse to disclose communications made between them during their marriage, thus protecting their privacy with respect to their marriage. The protection guaranteed by this provision is similar to English Common Law protection of confidentiality in marital relations.¹⁶⁶⁹ It must be noted that the privilege offered by section 198 (2) does not apply a where marriage has been dissolved or annulled by a competent court.¹⁶⁷⁰ However it has been observed that there are “special statutory provisions”¹⁶⁷¹ in South Africa by virtue of which marital privilege may be extended to ex-spouses.

Section 199 of the Criminal Procedure Act also allows a husband or wife to refuse to answer questions in circumstances in which his or her spouse would be entitled to claim privilege.¹⁶⁷² It is submitted that the protection offered by this provision is very limited as

¹⁶⁶⁷ Ibid.

¹⁶⁶⁸ See *S v Bosman* 1998 (2) SA 485 (A); *S v Kleinschmidt* 1980 (1) SA 852 (A); *S v Heyman* 1966 (4) SA 598 (A) See generally L.H. Hoffmann & D.T. Zeffert *The South African Law of Evidence* (1998) at 241.

¹⁶⁶⁹ *Argyll v Argyll* [1965] 1 All ER 611; [1967] Ch 308. Cf above Chapter 3.

¹⁶⁷⁰ Section 198(2).

¹⁶⁷¹ Hoffmann & Zeffert op cit at 245.

it merely gives a husband or wife the discretion to protect or refrain from protecting the other party's privacy, and does not impose any obligation to protect such privacy.

Chapter 2 of the Act provides for powers of search and seizure of certain articles. Section 21 of the Act however prohibits unauthorised searches and seizures and provides that a search must be authorised by a duly prepared search warrant.¹⁶⁷³ The Act further specifies the circumstances under which a search or seizure may be conducted without a search warrant.¹⁶⁷⁴ These provisions act as a safeguard against arbitrary and unregulated searches. For our purposes, it is unclear whether a warrant will be required to search information contained in a computer.¹⁶⁷⁵ It has however been held to be an invasion of privacy for the police to seize a computer terminal without a warrant.¹⁶⁷⁶

7.1.2.1.5a Relevance to Internet Cafes

The provisions of Section 203 allowing the nondisclosure of incriminating evidence will be relevant in cases of information processed in Internet cafes. Similarly, Sections 198 and 199 protecting communications between husbands and wives will be relevant where the communications were processed in Internet cafes. The provisions on searches and

¹⁶⁷² See generally Hoffmann & Zeffert op cit at 245.

¹⁶⁷³ Section 21(2). See *S v Motloutsi* 1996 (1) SA 584 (C).

¹⁶⁷⁴ Section 22.

¹⁶⁷⁵ Cf *S v Motloutsi* supra . See also Buys op cit at 371.

¹⁶⁷⁶ See *S v Motloutsi* supra; Cf *S v Madiba & Anor* 1998 (1) BCLR 38 (D).

seizures will also be relevant for our purpose. Under Section 21 of the Criminal Procedure Act, it will be unlawful to conduct a search involving the seizure of computers or any other equipments or documents present on Internet café premises without a warrant unless one of the conditions specified for the conduct of a search or seizure without a warrant is fulfilled.

7.1.2.1.6 The Civil Proceedings Evidence Act¹⁶⁷⁷

The Civil Proceedings Evidence Act contains provisions that are similar to those contained in the Criminal Procedure Act for the protection of privacy in civil proceedings. Sections 14 and 42 of the Evidence Act makes the English Law as at 30th May 1961 applicable to civil proceedings in South Africa. The position therefore is that a witness is entitled to refuse to answer questions that may incriminate him or her in civil proceedings, as well as administrative and other proceedings. This includes proceedings involving penalties and forfeitures.¹⁶⁷⁸

In addition, Section 10 of the Civil Proceedings Evidence Act¹⁶⁷⁹ provides that for the right of a husband or wife not to be compelled to disclose communications made between

¹⁶⁷⁷ No 25 of 1965.

¹⁶⁷⁸ See *S v Lwane* 1966 (2) SA 433 (A). See also *R v Diedericks* 1957 (3) SA 661 (E). See generally Hoffmann & Zeffert at 237f.

¹⁶⁷⁹ 1965.

them during marriage. The protection provide by this section is analogous to English Common law protection of marital confidence.¹⁶⁸⁰

7.1.2.1.6a Relevance to Internet Cafes

As above, the provisions allowing the non- disclosure of incriminating evidence and of communications between spouses during marriage will be relevant where such information was processed in an Internet cafe.

7.1.2.1.7 Natal Law to Amend the Law of Evidence¹⁶⁸¹

Section 3 of the Natal Law provides that a woman is not bound to answer questions that tend to show that she is guilty of adultery or *Stuprum*.¹⁶⁸² Although this section of the law has been repealed by the Civil Proceedings Evidence Act,¹⁶⁸³ the privilege it confers will still be valid by virtue of section 42 of the Evidence Act¹⁶⁸⁴ which preserves the law that existed before the 30th of May 1961, where the Evidence Act does not make provisions for such cases.¹⁶⁸⁵

¹⁶⁸⁰ Cf *Argyll v Argyll* supra. Cf above Para 3.2.1.1.1.

¹⁶⁸¹ Evidence Law No 5 of 1870.

¹⁶⁸² “Any sexual intercourse other than between husband and wife.” See Hoffmann & Zeffert op cit at 246.

¹⁶⁸³ Act 25 of 1965.

¹⁶⁸⁴ Ibid.

¹⁶⁸⁵ See generally Hoffmann & Zeffert op cit at 246.

This provision protects the disclosural privacy of persons in civil proceedings, with regard to their sexual relationships.¹⁶⁸⁶ This provision is however applicable only to civil actions in Kwazulu-Natal. Where however a party refuses to disclose information on the basis of this provision, the court may draw an unfavourable inference.¹⁶⁸⁷ It is submitted that drawing an unfavourable inference as a result of refusal to disclose information by an accused person is a violation of the right to fair trial and presumption of innocence guaranteed in Section 35 (3)h of the Constitution.¹⁶⁸⁸ It has also been observed that the drawing an unfavourable inference may serve to defeat the purpose of the provision.¹⁶⁸⁹

7.1.2.1.7a Relevance to Internet Cafes

Again, this provision will only be relevant for the protection of information relating to sexual relations outside marriage processed in Internet cafes. It is however affirmed that allowing the court to draw an unfavourable conclusion from non-disclosure is an unfair and prejudicial provision which weakens and may effectually defeat the essence of the protection sought to be given.

7.1.2.1.8 The Copyright Act¹⁶⁹⁰

¹⁶⁸⁶ Cf Section 211 of the Nigerian Evidence (Cap 112 LFN), which provides a similar protection for the prosecutrix in rape cases; Cf below Para 5.2.2.1.4.

¹⁶⁸⁷ *Thomas v Thomas* 1949 (1) SA 445 (A).

¹⁶⁸⁸ Act 108 of 1996.

¹⁶⁸⁹ Hoffmann & Zeffert op cit at 246.

¹⁶⁹⁰ Act 98 of 1978 as amended.

The South African Copyright Act provides protection for original literary,¹⁶⁹¹ musical,¹⁶⁹² and artistic¹⁶⁹³ works. “Artistic works” as defined in the Act, includes paintings, drawings, sculptures and photographs.¹⁶⁹⁴ Copyright protection is also available under the Act for sound recordings,¹⁶⁹⁵ as well as computer programs.¹⁶⁹⁶ Thus where privacy invasion involves unlawful use or publication of any form of information (i.e. literary work, artistic work, sound recording e.t.c) that is protected by copyright law, there will be liability for such privacy invasion under the relevant copyright laws.

7.1.2.1.8a Relevance to Internet Cafes

Copyright laws will only be relevant for our purpose where the form in which information exists is protected by copyright laws and the author or creator has taken the necessary measures to obtain copyright protection in respect of the information (form). Thus where copyright –protected information, such as a poem, photograph, personal recording or information contained in a computer program is published via an Internet café, the author or original creator(s) will be able to bring action for copyright infringement in respect of such publication.

¹⁶⁹¹ Chapter 1(1)(a).

¹⁶⁹² Chapter 1(1)(b).

¹⁶⁹³ Chapter 1(1)(c).

¹⁶⁹⁴ Chapter 1(1)(d).

¹⁶⁹⁵ Chapter 1(1)(e).

¹⁶⁹⁶ Chapter 1(1)(i).

7.1.2.1.9 The National Credit Act¹⁶⁹⁷

Chapter 4 of the National Credit Act (NCA) contains provisions protecting privacy and data. Part B deals with confidentiality, personal information and consumer credit records. The Act provides for a right to confidential treatment of ‘confidential information’ received, compiled, retained or reported in terms of the Act.¹⁶⁹⁸ “Confidential information” is defined in the Act as “personal information that belongs to a person and is not generally available to or known by others.”¹⁶⁹⁹ Section 68 provides that confidential information must be used only for a lawful purpose¹⁷⁰⁰ and must be disclosed only to the consumer or prospective consumer (the person to whom the information relates) or to a third party where required by law or directed by court order or on the instructions of the consumer/prospective consumer.¹⁷⁰¹

7.1.2.1.9a Relevance to Internet Cafes

The provisions of the NCA creating a right to confidential treatment of confidential information¹⁷⁰² will be instructive for the protection of information processed in Internet

¹⁶⁹⁷ No 34 of 2005.

¹⁶⁹⁸ Section 68.

¹⁶⁹⁹ Section 1.

¹⁷⁰⁰ Section 68(1)(a).

¹⁷⁰¹ Section 68(1)(b).

¹⁷⁰² Section 68.

cafes. Since Internet café personnel keep custody of (retain) information that may be regarded as confidential information under the Act,¹⁷⁰³ it is submitted that the provisions of Section 68 creating a duty of confidence be applied to Internet café staff with regard to personal information relating to their customers that is not generally available to or known by others.¹⁷⁰⁴ Thus, where personal information that is not generally available to others is processed in an Internet café and subsequently unlawfully used or disclosed to a third party by a member of staff in that Internet café, there will be liability for such disclosure.

7.1.2.1.10 The Consumer Protection Bill¹⁷⁰⁵

The Consumer Protection Bill contains provisions dealing extensively with the promotion and protection of the economic interests (as well as the health and safety) of consumers.¹⁷⁰⁶ “Consumer” is defined in the Act depending on the context, as a person to whom goods and services are advertised, offered, supplied, sold, leased, or delivered, in the course of business,¹⁷⁰⁷ a user of such goods or a recipient or beneficiary of such

¹⁷⁰³ Section 1.

¹⁷⁰⁴ Ibid.

¹⁷⁰⁵ Government Gazette No 28629; 15 March 2006.

¹⁷⁰⁶ See the Preamble to the Act.

¹⁷⁰⁷ Section 1(a).

services,¹⁷⁰⁸ or any person who has entered into an agreement or transaction with a supplier.¹⁷⁰⁹

Part B¹⁷¹⁰ of the Act deals with the right to confidentiality and privacy. Section 12 imposes a duty of confidentiality on persons who receive, compile, retain or report confidential information relating to consumers or prospective consumers. It prohibits the disclosure of such information and specifies the conditions under which such information may be disclosed.¹⁷¹¹

“Confidential information” is defined in the Act¹⁷¹² to include information concerning a person’s identity including name, date of birth, identity number, marital status, family relationships, past and current addresses and other contact details.¹⁷¹³ It also includes information relating to a person’s education, employment, career, professional or business history,¹⁷¹⁴ consumer history,¹⁷¹⁵ financial history¹⁷¹⁶ and “other personal information by which a person may be identified that belongs to a person and is not

¹⁷⁰⁸ Section 1(b).

¹⁷⁰⁹ Section 1(c).

¹⁷¹⁰ Sections 12 -15.

¹⁷¹¹ Section 12 (1) (b) which permits the disclosure of information only to the person to whom the information relates or to another person when, and to the extent required by law. Section 12 (2) provides for written direction from the consumer or prospective consumer for the release of confidential information under Section 1.

¹⁷¹² Part A Section 1.

¹⁷¹³ Section 1(a)(i).

¹⁷¹⁴ Section 1(a)(ii).

¹⁷¹⁵ Section 1(a)(iii).

¹⁷¹⁶ Section 1(a)(iv).

generally available to or known by others.”¹⁷¹⁷ It is submitted that the definition of confidential information is and

Section 13 prohibits the use of personal information for promotional, marketing or other related purposes. It also prohibits the initiation, sponsoring, promotion of, or intentional participation in, any activity whose main objective is the accumulation of confidential information or other identifying information relating to consumers.¹⁷¹⁸ Section 14 provides for the right of consumers to restrict unwanted telecommunication.

7.1.2.1.10a Relevance to Internet Cafes

The broad definition of consumer in the Act covers customers in Internet cafés both as persons to whom services are supplied¹⁷¹⁹ and as beneficiaries of such services.¹⁷²⁰ Since basic personal information as well as other categories of information classified in the Act as confidential (such as information relating to career, employment as well as other information by which a person may be identified)¹⁷²¹ is often processed in Internet cafes, Section 12 of the Act will apply. As such, a duty of confidentiality will exist between Internet café personnel and customers and there will be liability for unlawful disclosure

¹⁷¹⁷ Section 1(b).

¹⁷¹⁸ Section 13(4).

¹⁷¹⁹ Section 1(a). Cf above Para 7.1.2.1.10.

¹⁷²⁰ Section 1(b).

of any information that amounts to confidential information under the Act, where such information relates to customers and is disclosed by Internet café personnel.

7.1.2.2 Statutory Protection of Data in South Africa

Although there is no Data Protection Act in South Africa, a proposal has been made for a comprehensive Data Protection Act for South Africa.¹⁷²² In this regard, the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (COE Convention),¹⁷²³ and the 1981 Organisation for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data¹⁷²⁴ have been identified as being instrumental in the development and enactment of data legislation in many countries.¹⁷²⁵

From the standards set in the Convention and the Guidelines,¹⁷²⁶ certain elements have been identified as the common principles of data protection that represent the core of both legislative regulation and self-regulation control.¹⁷²⁷ These different elements have been crystallised into the following eight principles, which have been proposed for adoption in

¹⁷²¹ Part A Section 1. Above Para 7.1.2.1.10.

¹⁷²² See generally the South African Law Reform Commission Discussion Papers "Discussion Paper 109 Project 124" at <http://www.doj.gov.za/salrc/dpapers.htm> Accessed June 2007.

¹⁷²³ COE- ETS No 108 1981.

¹⁷²⁴ OECD Guidelines 1981.

¹⁷²⁵ See the SALRC Discussion Papers op cit at Chapter 4. See also The South African Law Reform Commission Issue Papers "Summary of Proposals and Questionnaire Issue Paper 24" at http://www.doj.gov.za/salrc/ipapers/ip24_prj124/ip24_prj124_2003_sum_ques.pdf Accessed June 2007.

¹⁷²⁶ Ibid. See also Currie Iain "The NCA and the Proposed Protection of Personal Information Act" at <http://wwwserver.law.wits.ac.za/mi/privacy/nationalcreditact.htm> Accessed June 2007.

a South African data protection Act: Processing Limitation (Fair and lawful processing), Purpose Specification, Further Processing Limitation, Information Quality, Openness, Security Safeguards, Individual Participation and Accountability.¹⁷²⁸ It is noteworthy that the principles affirmed and suggested for inclusion in the South African data Act are analogous to those identified by Neethling¹⁷²⁹ as the general principles that should form the basis of data protection law. They have also subsequently been discussed, affirmed and recommended for inclusion in a South African Data Act.¹⁷³⁰

Finally, the following aspects of data protection have been included in the scope of the Law Reform Commission's investigation:

- (i) automatic and manual processing of data
- (ii) information pertaining to both natural and juristic persons
- (iii) information kept by both the public and private sector, and
- (iv) sound and image data.¹⁷³¹

At present, some protection can be found for data in the provisions of some statutes. The following statutes, which provide for the giving of information by individuals, also have

¹⁷²⁷ See SALRC Discussion Papers op cit at Chapter 4 Para 1.2.23.

¹⁷²⁸ Cf SALRC Discussion Papers op cit at Chapter 4 Para 4.2.8. See also Part A of the proposed South African Protection of Personal Information Act 2005.

¹⁷²⁹ Cf Neethling *Persoonlikheidsreg* (1985) at 336-337 cited in Roos op cit at 650.

¹⁷³⁰ See generally Roos op cit especially at chapters 3 and 4, at 650- 652 and 720- 721.

¹⁷³¹ See Chapter 2 of the proposed South African Protection of Personal Information Act 2005.

safeguards to protect information so obtained: the Electronic Communications and Transactions Act,¹⁷³² the Statistics Act,¹⁷³³ and the Income Tax Act.¹⁷³⁴ In addition, some of the Provisions of the Promotion of Access to Information Act,¹⁷³⁵ the Criminal Procedure Act,¹⁷³⁶ the Regulation of Interception of Communications and Provision of Communication-Related Information Act,¹⁷³⁷ the National Credit Act¹⁷³⁸ and the Consumer Protection Bill¹⁷³⁹ contain provisions protecting data. The relevant portions of these Acts will be examined below.

7.1.2.2.1 The Electronic Communications and Transactions Act¹⁷⁴⁰

This Act regulates electronic commerce and its provisions apply to the collation, processing storage and disclosure of data.¹⁷⁴¹ The purpose of the Act is to promote access to electronic communications and the prevention of abuse of information systems.¹⁷⁴² The Act purports to provide for legal procedural technical means to ensure the data security

¹⁷³² Act 25 of 2002.

¹⁷³³ Act 68 of 1977.

¹⁷³⁴ Act 66 of 1976.

¹⁷³⁵ Act 2 of 2000.

¹⁷³⁶ Act 51 of 1977.

¹⁷³⁷ Act 70 of 2002.

¹⁷³⁸ No 34 of 2005.

¹⁷³⁹ Government Gazette No 28629; 15 March 2006.

¹⁷⁴⁰ Act 25 of 2002.

¹⁷⁴¹ See Preamble to the Act.

for electronic commerce. In this regard, the following key elements have been identified¹⁷⁴³ as necessary: authentication,¹⁷⁴⁴ confidentiality,¹⁷⁴⁵ integrity,¹⁷⁴⁶ and non-repudiation.¹⁷⁴⁷

The Act protects the privacy of natural persons where information regarding them has been obtained through electronic transactions after the coming into effect of the Act.¹⁷⁴⁸

The Act also lays down nine principles to be followed by data controllers with regard to the electronic collection of personal information.¹⁷⁴⁹ These principles are in line with fair information principles.¹⁷⁵⁰

In this regard, the Act provides for the obtaining of permission from data subjects for collection of personal data.¹⁷⁵¹ It also provides that data must only be collected for a necessary and lawful purpose,¹⁷⁵² and provides that the purpose for data collection must be disclosed to the concerned data subject.¹⁷⁵³ The Act further provides that data

¹⁷⁴² Ibid.

¹⁷⁴³ See Green Paper on Electronic Commerce for South Africa (2000) Chapter 7 at http://www.polity.org.za/html/govdocs/green_papers/greenpaper/theme2.html#7 Accessed December 2004.

¹⁷⁴⁴ Defined in the paper as “securing the identities of the parties to a transaction”.

¹⁷⁴⁵ Defined as “ensuring that information is kept private”.

¹⁷⁴⁶ Defined as “ensuring that the information or process has not been modified or corrupted without detection”.

¹⁷⁴⁷ Defined as “ensuring that neither party can refute that the transaction occurred”.

¹⁷⁴⁸ Chapter VIII. See also section 50.

¹⁷⁴⁹ Section 51.

¹⁷⁵⁰ See R Buys (ed) *Cyberlaw@ SA II: The Law of the Internet in South Africa* (2004) at 379 – 380.

¹⁷⁵¹ Section 51(1).

¹⁷⁵² Section 51(2).

collected must be used for the purpose specified,¹⁷⁵⁴ and makes provisions to ensure that data is not kept for longer than necessary.¹⁷⁵⁵

The Act also contains some protection with regard to cryptography. Chapter five of the Act deals with cryptography providers and Section 29 provides for a register of cryptography providers. Section 31 prohibits disclosure of information contained in Section 29 to persons other than employees of the department responsible for keeping the register except under the circumstances specified in subsection 2.¹⁷⁵⁶

In addition, Section 29(1) provides that a cryptography provider is not required to disclose confidential information about its cryptography products or services. The provisions of Section 31 and Section 29(1), guarantee privacy protection in respect of information regarding the use of cryptography services by individuals. This provision constitutes legal support for the use of technical extra-legal means for the prevention of unlawful access to personal information.

Section 53 provides for certain classes of information of importance to national security and the well-being of citizens to be declared critical data. Section 56 imposes restrictions

¹⁷⁵³ Section 51(3).

¹⁷⁵⁴ Section 51(4).

¹⁷⁵⁵ Section 51(5).

¹⁷⁵⁶ These include information disclosed:

- “(a) to a relevant authority investigating a criminal offence
- (b) to government agencies responsible for safety and security in South Africa pursuant to an official request
- (c) to a cyber inspector
- (d) pursuant to the relevant of the Promotion of Access to information Act 2002 and
- (e) for the purpose of civil proceedings relating to provision of cryptographic services.”

on disclosure of information contained in critical databases except under the circumstances in subsection 2.¹⁷⁵⁷

However, individual protection of personal data guaranteed by the Act is limited where parties have entered into contractual relations.¹⁷⁵⁸ In this regard, the Act provides that the rights and obligations of the parties in respect of a breach of the principles in section 51 of the Act are governed by the terms of agreement between them.¹⁷⁵⁹ The Act is also limited in terms of the provision that states that it is only applicable to personal information obtained through electronic transactions.¹⁷⁶⁰

7.1.2.2.1a Relevance to Internet Cafes

The Electronic Communications and Transactions Act¹⁷⁶¹ will be of great utility for the protection of privacy where personal information is released for the purchase of goods or delivery of services via the Internet. In the present day, this has become commonplace in developed economies such as the United Kingdom, the United States, Germany and Canada to mention a few. Such transactions more often than not require the giving of some personal as well as financial information online. Considering the damage that may

¹⁷⁵⁷ Section 56(a) – (e). (See above).

¹⁷⁵⁸ Part 2 of the Act.

¹⁷⁵⁹ Section 21.

¹⁷⁶⁰ Section 50.

¹⁷⁶¹ Act 25 of 2002.

occasioned to privacy (as well as finances) by the misuse of such information via the Internet, a law for the regulation of such transactions is necessary and of immense value for the protection of privacy.

The Act also contains provisions that are relevant for the protection of data in general as well as for information processed in Internet cafes. In this regard, the nine principles in Section 51 of the Act, to be followed by data controllers are the same in essence as the OECD principles. The observations in this work¹⁷⁶² regarding the utility of the OECD principles for the protection of data in Internet cafes will thus apply

The Act will also be useful for the protection of electronic mail in Internet cafes where there is an agreement between the Internet café owner (and his or her staff) and the customer as to the confidentiality of information processed through the Internet café.

7.1.2.2.2 The Statistics Act¹⁷⁶³

The Statistics Act regulates the collection, production and dissemination of official and other statistics, including the conducting of the census.¹⁷⁶⁴ It defines statistics and other relevant terms.¹⁷⁶⁵ Statistics are defined as:

¹⁷⁶² Above at Para 3.2.3.21 and below at Chapter 9.

¹⁷⁶³ Act 66 of 1976.

¹⁷⁶⁴ See the Preamble.

¹⁷⁶⁵ Section 1-Definitions

“aggregated numerical information relating to demographic, economic, financial, environmental, social or similar matters at national, provincial or local level, which is compiled and analysed according to relevant scientific and statistical methodology.”

The Act applies to both natural and juristic persons.¹⁷⁶⁶ Certain provisions of the Act protect data directly. Section 3(2) of the Act provides for the protection of the confidentiality of information provided pursuant to the Act. Section 16 provides for the duty to answer questions. It states that:

“Every person ... must to the best of his or her knowledge and belief and subject to the right to dignity and privacy, answer, when so required, all questions put orally or in writing in terms of subsection 1.”¹⁷⁶⁷

Section 17 of the Act forbids the disclosure of information relating to an individual, household, organ of state, business, or any other organisation, to any person except under circumstances prescribed by the Act.¹⁷⁶⁸ The Act further provides that information collected must be relevant, accurate, reliable and timeous,¹⁷⁶⁹ as well as objective.¹⁷⁷⁰ It also provides that such information must be disseminated impartially.¹⁷⁷¹

¹⁷⁶⁶ Section 1.

¹⁷⁶⁷ Subsection 1 authorises the Statistician-General and other officials recognised under the Act to ask questions in the performance of their duties under the Act.

¹⁷⁶⁸ Section 17(2) & (3).

¹⁷⁶⁹ Section 3(2)(a).

¹⁷⁷⁰ Section 3(2)(b).

The Act provides for a Statistician-General to administer the Act¹⁷⁷² and a Council¹⁷⁷³ to advise the Statistician-General, and contains specific and detailed provisions on the duties and powers of these persons or organs.¹⁷⁷⁴ Very significantly, the Act provides for information collected to be in accordance with appropriate national and international standards and classifications.¹⁷⁷⁵

The Act prescribes penalties for violations of the provisions of the Act¹⁷⁷⁶ by officials. Such violations include, among others specified in section 18, the obtaining or seeking of information that they are not authorised to obtain,¹⁷⁷⁷ wilfully disclosing data or information obtained in the course of their employment to persons not authorised to receive the information¹⁷⁷⁸ and other forms of misuse of information.¹⁷⁷⁹

7.1.2.2.2a Relevance to Internet Cafes

¹⁷⁷¹ Section 3(2)(d).

¹⁷⁷² Section 7(1)(a)

¹⁷⁷³ Section 8.

¹⁷⁷⁴ Section 7 –Duties and Powers of Statistician-General, Section 13- Duties and Powers of Council.

¹⁷⁷⁵ Section 3(2)(f).

¹⁷⁷⁶ Section 18.

¹⁷⁷⁷ Section 18(1)(b).

¹⁷⁷⁸ Section 18(1)(e). This provision also protects the right to privacy.

¹⁷⁷⁹ Section 18(1)(f).

This Act may not be of much utility for protection of information processed in Internet cafes in particular as it relates explicitly to the gathering and processing of information that may be classified as official records and statistics.

7.1.2.2.3 The Income Tax Act¹⁷⁸⁰

The Department of Inland Revenue requires certain highly confidential information with regard to a person's financial position, property holdings, family, and so forth in order to assess the taxable income of the individual in the society.¹⁷⁸¹ To ensure the protection of privacy, the Income Tax Act provides that an income tax official:

“Shall preserve and aid in preserving secrecy with regard to all matters that may come to his knowledge in the performance of his duties ... and shall not communicate any such matter to any person whatsoever, other than the taxpayer concerned or his lawful representative.”¹⁷⁸²

Section 4(2A) prohibits the publication or making known of information concerning tax matters of a taxpayer or class of taxpayers except when this is required in the line of duty under the Commissioner. In addition, to safeguard the privacy of persons obliged to submit such returns including taxpayers, employees of the department are required to

¹⁷⁸⁰ Act 58 of 1962.

¹⁷⁸¹ Section 69; Section 74 (A-B).

¹⁷⁸² Section 4. See *Ferela (Pty) Ltd & ors v Commissioner for Inland Revenue & ors* 1998 (4) SA 275 (T); *Estate Dempers v SIR* 1977 (3) SA 410 (AD). See also *Welz v Hall* 1996 (4) SA 1073 (C).

take an oath of secrecy.¹⁷⁸³ The utility of the secrecy provisions in enhancing the administrative capabilities of revenue authorities in present times has however been questioned.¹⁷⁸⁴

7.1.2.2.3a Relevance to Internet Cafes

Again, this Act is specifically relevant for the protection of tax-related information and its provisions protecting information are directed to officials involved in the processing of such information. These provisions will therefore be of no direct application to Internet café privacy protection except, perhaps, to underline the confidential nature of financial information and inform the suggestion of strict measures for its protection in Internet cafes.

7.1.2.2.4 The Promotion of Access to Information Act¹⁷⁸⁵

Many of the provisions of the Promotion of Access to Information Act protecting privacy¹⁷⁸⁶ may also be used for the protection of data. Generally, Section 9 of the Act which makes consideration of the constitutional right to privacy relevant in determining

¹⁷⁸³ Section 4(2). See *Hyundai Motor Distributors (Pty) Ltd & ors v Smit NO & ors* 2000 (2) SA 934 (T). Contra *Sackstein v South African Revenue Service* 2000 (2) SA 250 (SE).

¹⁷⁸⁴ R G Bricout “ The Preservation of Secrecy Provisions: Still Worth It?” (2002) *Acta Juridica* 247. See pp 280 - 281.

¹⁷⁸⁵ No 2 of 2000. (The draft form of the Access to Information Act (known as the Open Democracy (Act Draft) Bill 1998 Govt Gazette 18381 no 1514; {Bill 67 of 1998}) highlighted provisions for data protection which have been incorporated into the Act.)

¹⁷⁸⁶ Section 12. See Sections 30, 34-43, 63-69; Cf above Para 7.1.2.1.1.

whether or not to allow access to information will also protect data. In addition, the provisions of Parts 2 and 3,¹⁷⁸⁷ which specify certain grounds on which access to records may be refused, will be relevant. These include the protection of: the privacy of a third party who is a natural person,¹⁷⁸⁸ commercial information of a third party¹⁷⁸⁹ or private body,¹⁷⁹⁰ certain records of the South African Revenue Service,¹⁷⁹¹ information supplied in confidence¹⁷⁹² and the safety of the individual and of property.¹⁷⁹³ Thus, information which may be classified as data and pertains to any of the above will be protected under the Act.

The provisions allowing for rights of correction by persons affected by incorrect records¹⁷⁹⁴ and those protecting health records,¹⁷⁹⁵ certain official records and privileged information¹⁷⁹⁶ will also be applicable for the protection of data.

7.1.2.2.4a Relevance to Internet Cafes

¹⁷⁸⁷ Part 2, chapter 4; part 3, chapter 4.

¹⁷⁸⁸ Section 34 & Section 63.

¹⁷⁸⁹ Section 36 & Section 64.

¹⁷⁹⁰ Section 68.

¹⁷⁹¹ Section 35.

¹⁷⁹² Section 37 & Section 65.

¹⁷⁹³ Section 38 & Section 66.

¹⁷⁹⁴ Section 88.

¹⁷⁹⁵ Section 30 & Section 61.

¹⁷⁹⁶ Section 12, Section 41. See also *CCII Systems (Pty) Ltd v Fakie NNO* 2003 (2) SA 325 (T).

It is submitted that Section 9 of the Act will be of much utility as a basic foundational guide for determining whether to allow or deny access to any information contained in Internet café depositories. In effect, if access to information or data contained in any Internet café depository will constitute an infringement on the right to privacy as provided for in the Constitution, such access will be denied.

As in the case of privacy protection,¹⁷⁹⁷ the provisions specifying the grounds for the refusal of access to records¹⁷⁹⁸ will also be instructive for determining categories or genre of information regarding which access may be denied in Internet cafes. Thus, access to personal information contained in Internet café premises or equipment will be denied for the protection of: privacy of a third party who is a natural person;¹⁷⁹⁹ commercial information of a third party;¹⁸⁰⁰ commercial information of a private body,¹⁸⁰¹ information supplied in confidence;¹⁸⁰² safety of the individual and of property¹⁸⁰³ and the protection of health records.¹⁸⁰⁴

¹⁷⁹⁷ Cf above Para 7.1.2.1.1a.

¹⁷⁹⁸ Part 2, chapter 4; Part 3, chapter 4.

¹⁷⁹⁹ Section 34 & Section 63.

¹⁸⁰⁰ Section 36 & Section 64.

¹⁸⁰¹ Section 68.

¹⁸⁰² Section 37 & Section 65.

¹⁸⁰³ Section 38 & Section 66.

¹⁸⁰⁴ Section 30 & section 61.

7.1.2.2.5 The Criminal Procedure Act¹⁸⁰⁵

This Act provides for the taking, by, or at the request of¹⁸⁰⁶ a police official, of the fingerprints, palm-prints and footprints of any person arrested on a criminal charge, or convicted of a crime.¹⁸⁰⁷ Where such a person is acquitted, or his sentence set aside, or should the state decline to prosecute, then the records of fingerprints, palm-prints or footprints must be destroyed.¹⁸⁰⁸ The Criminal procedure Act also contains provisions regarding the protection of rape survivors and the protection of young children from having their identity disclosed in criminal proceedings.

7.1.2.2.5a Relevance to Internet Cafes

The provisions of the Criminal Procedure Act that protect data will only be relevant for the protection of information in Internet cafes in the unlikely event that information protected under the CPA is processed and or disclosed via an Internet café.

7.1.2.2.6 The Regulation of Interception of Communications and Provision of Communication- Related Information Act¹⁸⁰⁹

¹⁸⁰⁵ Act 51 of 1977.

¹⁸⁰⁶ Section 37(2).

¹⁸⁰⁷ Section 37(1)(a).

¹⁸⁰⁸ Section 37(5).

¹⁸⁰⁹ Act 70 of 2002.

This Act regulates the interception of certain communications, the monitoring of signals and the provision of certain communication-related information.¹⁸¹⁰ Interception is defined in the Act, as the

“aural or other acquisition of the contents of any communication through the use of any means including an interception device so as to make some or all of the contents of a communication available to a person other than the sender or the recipient or intended recipient of that communication”

Interception in the Act includes monitoring, viewing, examination, inspection, diversion of any indirect communication. The Act prohibits the interception of communication¹⁸¹¹ except in certain circumstances provided for under the Act.¹⁸¹² It also disallows the “prohibition of real time¹⁸¹³ or archived¹⁸¹⁴ communication-related information”.¹⁸¹⁵ In addition, the Act provides for the obtaining of interception directions and warrants in

¹⁸¹⁰ See preamble to the Act.

¹⁸¹¹ Part 1 Section 2.

¹⁸¹² Part 1 Sections 3 - 11.

¹⁸¹³ “Real-time communication- related information” is defined in the Act as “communication-related information which is immediately available to a telecommunication service provider.” See Section 1.

¹⁸¹⁴ “ communication-related direction” is defined as any communication-related information in the possession of a telecommunications service provider, which is being stored by the telecommunications service provider in terms of section 30 (1) b of the Act under specified circumstances. See section 1.

¹⁸¹⁵ Part 2 Section 12.

order to intercept communications.¹⁸¹⁶ The Act defines communication in terms of both direct and indirect communication.¹⁸¹⁷

Chapter 5 of the Act deals with the interception capability of telecommunication services and the storing of communication-related information. Section 42 of the Act prohibits the disclosure of information and provides for exceptions to this.¹⁸¹⁸ The Act applies to telecommunication service providers, postal service providers and Internet service providers.¹⁸¹⁹ It also applies in respect of business activities conducted by individuals, private or public bodies.¹⁸²⁰

7.1.2.2.6a Relevance to Internet Cafes

The Regulation of Interception of Communications and Provision of Communication-Related Information Act will be useful for the protection of information relating to customers' communication where such information is immediately available to Internet

¹⁸¹⁶ Chapter 3 Section 16.

¹⁸¹⁷ Section 1.

“Direct communication” is defined in the Act as oral communication between two or more persons which occurs in the immediate presence of all the persons participating in that communication . It also includes utterances by a person who is participating in an indirect communication where the utterance is audible to another who is in the immediate presence of the person participating in the indirect communication.

“Indirect communication” includes the transfer of messages in whole or in part by means of a postal service or a telecommunication system.

¹⁸¹⁸ Section 43, which provides for the disclosure of information by an authorised person for the performance of official duties. See also Section 46.

¹⁸¹⁹ Section 1.

¹⁸²⁰ Ibid.

café personnel,¹⁸²¹ such as facts or personal information of which they are aware. It will also be useful for the protection of information related to customers' communication, which is being stored by the service provider, such as information contained on the hard drives of their computers.¹⁸²²

The RICPCRIA protects information sent electronically and through a postal service provider.¹⁸²³ As such, it will be useful where for instance, any Internet café personnel or a third party intercepts mail sent by customers, either in the process of sending such mail electronically, or where mail that has been printed out is manually handled and intercepted. It will also be useful for the regulation of the interception of mail that is sent through a postal service provider.

7.1.2.2.7 The National Credit Act¹⁸²⁴

The provisions of Section 68 of the National Credit Act creating a right to confidential treatment of confidential information¹⁸²⁵ will, in protecting privacy, also be applicable for the protection of data. More specifically, the provisions of the Act regulating credit bureau information (Sections 70 -73) are particularly relevant. Sections 70 deals with the

¹⁸²¹ See Section 1.

¹⁸²² Ibid.

¹⁸²³ Section 1.

¹⁸²⁴ No 34 of 2005.

¹⁸²⁵ Cf above Para 7.1.2.1.9.

protection of consumer credit information which is defined in the Act to include a person's credit history,¹⁸²⁶ financial history,¹⁸²⁷ education, employment, career, professional or business history¹⁸²⁸ as well as identity including name, date of birth, marital status, contact details and related matters.¹⁸²⁹ Section 70 provides for a duty to take reasonable steps to verify the accuracy of consumer credit information.¹⁸³⁰ It also limits access to and use of credit bureaux data to persons who require it for a prescribed purpose or a purpose contemplated in the Act.¹⁸³¹

Section 71 provides for the removal of record of debt adjustment or judgement. This entails the removal of all records and information, relating to a debt. Section 71 also provides for the expungement of all information or records relating to the judgement. Section 72 provides for a right to access and challenge credit records and information while Section 73 provides for the verification, review and removal of all credit information. By virtue of Section 73, data cannot be retained indefinitely; it must be verified, reviewed and removed in such manner and within such time as may be prescribed by the Minister.¹⁸³²

¹⁸²⁶ Section 70(1)(a).

¹⁸²⁷ Section 70(1)(b).

¹⁸²⁸ Section 70(1)(c).

¹⁸²⁹ Section 70(1)(d).

¹⁸³⁰ Section 70(2)(c).

¹⁸³¹ Section 70(2)(g).

¹⁸³² Section 73(1)(a).

7.1.2.2.7a Relevance to Internet Cafes

The provisions of the National Credit Act regulating consumer credit information are not directly applicable to Internet café personnel (for example, the verification by Internet café personnel of the accuracy of information processed by customers as per section 70 (2)(c) will be impracticable and may constitute privacy invasion). However, in line with Section 73, it is submitted that provisions generally prohibiting the indefinite retention of personal data relating to others and specifying the maximum duration for retention and the method of removal of such data should be enacted for Internet cafes.

As in the case of privacy protection,¹⁸³³ Section 68 of the National Credit Act will also be applicable for the protection of data. Thus where personal information amounting to data is processed in an Internet café and subsequently unlawfully used or disclosed to a third party, there will be liability for the unlawful disclosure.

7.1.2.2.8 The Consumer Protection Bill¹⁸³⁴

The provisions of the Consumer Protection Bill dealing with privacy are also applicable for the protection of data. The definition of confidential information¹⁸³⁵ in the Act covers information that may be regarded as data and in respect of which Section 12 of the Act will apply. Thus there will be liability for the unlawful disclosure of the following forms

¹⁸³³ Cf Para 7.1.2.1.9a

¹⁸³⁴ Government Gazette No 28629; 15 March 2006.

of data; Information relating to an Internet café user's name, date of birth, identity number, marital status, address, contact details,¹⁸³⁶ or information relating to financial,¹⁸³⁷ employment, professional, business¹⁸³⁸ or consumer history,¹⁸³⁹ and other personal information by which customers may be identified.

7.1.2.2.8a Relevance to Internet Cafes

Where personal information such as the name, date of birth, race, marital status, employment history, consumer history, financial history, or other data relating to a customer is disclosed by Internet café personnel, there will be liability for such unlawful disclosure under the provisions of the Consumer Protection Bill.

7.1.3 Conclusion on Statutory Protection of Privacy and Data in South Africa

The South African Constitution provides general and broad-based protection for the right to privacy for both natural and juristic persons, while specific statutes offer limited protection for privacy within their subject matter. It is submitted that, on the basis of Section 14 of the South African Constitution and Section 10 which provides for the right to dignity, coupled with the Common Law, which provides extensive protection in

¹⁸³⁵ Part A Section 1 (Cf above Para 7.1.2.1.10.)

¹⁸³⁶ Section 1(a)(i).

¹⁸³⁷ Section 1(a)(iv).

¹⁸³⁸ Section 1(a)(ii).

respect of miscellaneous acts amounting to injury to personality, there is ample and developable privacy protection legislation in South Africa.

Moreover, the flexibility of South African constitutional privacy law in allowing the prevailing *mores* to influence its development facilitates adaptability to societal needs and changes¹⁸⁴⁰ while consideration of relevant decisions in other legal systems with similar provisions broadens the scope of available legal resources, allows benefit from legal development outside South Africa and ultimately enhances legal development/reform.

Concerning data, the privacy protection provided for in the Constitution is applicable for the protection of data. Other Acts also provide limited protection for data within the scope of the subjects to which they relate. More specifically, the Criminal Procedure Act, the Income Tax Act, the Statistics Act, the National Credit Act and the Consumer Protection Bill all offer a measure of protection for data collected pursuant to these Acts.

The Statistics Act in particular offers detailed protection for data with respect to information processed by government organs. Its provisions cover the collection, use and disclosure of information, where such information qualifies as statistics,¹⁸⁴¹ and establishes appropriate organs for the administration of the Act.¹⁸⁴² It also provides

¹⁸³⁹ Section 1(a)(iii).

¹⁸⁴⁰ See also McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 118.

¹⁸⁴¹ See generally the Preamble and Section 2- Purpose of the Act.

¹⁸⁴² Section 7(1)(a) the Statistician-General, Section 8 The Council.

penalties¹⁸⁴³ for non-compliance with the Act. However, the provisions of the Statistics Act do not cover the gathering, use and disclosure of information by private individuals, or other bodies like the press, and government officials when they are not acting in the line of duty.

The Electronic Communications and Transactions Act, though of significant utility for automated transactions, therefore, relevant for the protection of electronic mail privacy in Internet cafes, contains inherent limitations regarding manually-kept or paper-based records and contractual situations.¹⁸⁴⁴

In the same vein, the provisions of the National Credit Act and the Consumer Protection Bill creating a duty of confidence in respect of information processed pursuant to these Acts provide generous privacy and data protection. However, the scope of application of the National Credit Act is limited to credit agreements between parties¹⁸⁴⁵ and the confidentiality provisions in the Act will only be binding on persons performing duties pursuant to the Act.¹⁸⁴⁶ Similarly, the Consumer Protection Bill will only apply to consumer information where transactions involving the exchange of goods and, or services or (a) credit agreement(s) have been contemplated or completed between

¹⁸⁴³ Section 18.

¹⁸⁴⁴ Cf above Para 7.1.2.2.1.

¹⁸⁴⁵ Cf Section 4 of the National Credit Act.

¹⁸⁴⁶ Cf Section 68.

parties.¹⁸⁴⁷ In effect, the privacy and data protection available by virtue of these Acts is limited in terms of the scope of application of the individual Acts.

In conclusion, while there is a good basis for the protection of data in South Africa flowing from the Constitution and different statutes, it is submitted that the enactment of a single Data Protection Act containing detailed provisions for the general protection of personal information and offering a broad foundation for the protection of data will be desirable.

7.1.3a Relevance to Internet Cafes

As shown above, while the South African Constitution will be useful in recognising and upholding general, as well as specified areas of, privacy and data protection rights,¹⁸⁴⁸ certain aspects of selected statutes¹⁸⁴⁹ will also be relevant for the protection of privacy and data in Internet cafes in South Africa. It is submitted that the basic privacy and data protection features embodied in the Constitution coupled with the principles gleaned from the select statutes as examined above, will be instructive in identifying principles to be included in any law for the protection of information processed in Internet cafes. These features will be discussed in further detail and applied below.¹⁸⁵⁰

¹⁸⁴⁷ Chapter 1 Section 5.

¹⁸⁴⁸ Cf above Paras 7.1.1.1 and 7.1.1.2.

¹⁸⁴⁹ Above Paras 7.1.2.1 and 7.1.2.2.

¹⁸⁵⁰ Below chapters 8 and 9.

7.2 Statutory Protection of Privacy and Data in Nigeria

7.2.1 Constitutional Protection

7.2.1.1 Constitutional Protection of Privacy in Nigeria

In Nigeria, the 1999 Constitution provides for the right to privacy in their family life.¹⁸⁵¹ Section 37 provides that “[T]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.” Although this provision provides a broad basis for the protection of the right to privacy in Nigeria, there has not been any direct judicial interpretation on it, thus there is no authority as to its application and the parameters within which it is applicable.

As to whether its provisions can be enforced against the government as well as against individuals i.e. both horizontally and vertically, Section 1(1) of the Constitution makes its provisions applicable to and binding on all authorities and persons in the Federal Republic of Nigeria. On this basis, it is submitted that it should be possible to bring action for the violation of any constitutional provision against individuals and government officials alike.¹⁸⁵²

¹⁸⁵¹ Section 37.

¹⁸⁵² However, there will be justification for acts amounting to privacy invasion where such acts are done pursuant to a validly made Act and within the limits of the authority conferred by the Act and/ or their office. For instance, where a police search is carried out pursuant to a warrant under circumstances where such intrusion would ordinarily constitute a breach of Section 37 which guarantees the privacy of citizens.

In *Tony Momoh v Senate*¹⁸⁵³ the courts upheld a journalist's right not to disclose the source of his information. The basis for the protection in this case was however the protection of the right to freedom of expression. Although the interest protected in this case is not one of the recognised privacy interests,¹⁸⁵⁴ the protection guaranteed in this case is comparable to that contained in Sections 198, 199 and 203 of the South African Criminal Procedure Act,¹⁸⁵⁵ which confers privileges on certain classes of persons to refuse to disclose admissible evidence.¹⁸⁵⁶

In addition to Section 37, the Nigerian Constitution also guarantees the right to dignity of the human person¹⁸⁵⁷ and the right to personal liberty.¹⁸⁵⁸ It is submitted that these should be read together with Section 37 of the Constitution to guarantee a broad basis for the protection of the right to privacy of the individual.¹⁸⁵⁹

7.2.1.1a Relevance to Internet Cafes

¹⁸⁵³ (1981) 1 NCLR 105.

¹⁸⁵⁴ Cf Prosser on the interests protected by privacy above at Para 1.1.

¹⁸⁵⁵ Act 51 of 1977 as amended.

¹⁸⁵⁶ Cf above Para 7.1.2.1.5.

¹⁸⁵⁷ Section 34.

¹⁸⁵⁸ Section 35. Cf above Para 1.1, where it is suggested that violations of the right to privacy constitute a threat to personal autonomy by giving others control over oneself. Thus restricting the exercise of one's liberty.

¹⁸⁵⁹ Cf the German courts' construction of Articles 1 and 2 of the German Basic Law (Above Para 5.1.1).

The constitutional guarantee of privacy will provide a solid basis for the general recognition of privacy rights as well as the protection of correspondence. As such, privacy protection will be available under the Constitution where, for instance, the plaintiff's e-mail is unlawfully read. It must be noted that in terms of the general right to privacy recognised under the Constitution, there will be no closed list of acts that will be covered.

7.2.1.2 Constitutional Protection of Data in Nigeria

Section 39 (3) of the Constitution provides that:

“[N]othing in this law shall invalidate any law that is reasonably justifiable in a democratic society for the purpose of preventing the disclosure of information received in confidence ... or regulating telephony, wireless broadcasting, television or the exhibition of cinematograph films.”¹⁸⁶⁰

This provision does not directly safeguard the protection of information or data, but it supports the enactment and enforcement of laws made for the purpose of protecting information received in confidence provided such laws are reasonably justifiable in a democratic society. This provision thus affirms and lends constitutionality to the Common Law breach of confidence laws for the protection of information.

¹⁸⁶⁰ Section 39 (3)(a).

However, this provision not sufficient for the protection of data as it does not confer any rights, nor impose liabilities for the protection of information or data. In essence, the provision does not provide any direct protection for data. Secondly, the scope of protection allowed by the provision is limited, as it applies only in respect of information received in confidence.

This creates a situation similar to the English law protection of information based on the principle of breach of confidentiality.¹⁸⁶¹ Thus, the provision will only be applicable in limited circumstances where a duty of confidence¹⁸⁶² is recognised. It is submitted that in the absence of any restricting clause in the provision, and in the light of contemporary technological advancements and the developments in English Common Law, this provision should be interpreted to allow liability for disclosure of information in circumstances where a relationship of confidence actually exists, as well as situations where, based on a fiduciary relationship between the parties, the law will impose a duty of confidentiality.¹⁸⁶³

The provision also permits the making of laws to regulate telecommunications in general, including cinematograph films, where such laws are reasonable and justifiable in a democratic society.¹⁸⁶⁴ Thus, laws made regarding the receiving and dissemination or

¹⁸⁶¹ Cf above Para 3.2.1.1.

¹⁸⁶² See Lord Goff of Chieveley in *Attorney General v Guardian Newspapers Ltd (No2)* (1990) 1 AC 109.

¹⁸⁶³ See *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804; *X Ltd v Morgan Grampian (Publishers) Ltd* [1991] 1 AC 1. Cf above Para 3.2.1.1.

¹⁸⁶⁴ Section 39(3)(a).

publication of information that forbid unlawful disclosure of data or information via wireless broadcasting, television or cinematograph films are constitutional. Again, this provision does not provide direct protection for data.

Apart from this provision, the Nigerian Constitution does not contain any direct provision on data protection and access to, or protection of, information in general. However, in *Theophilus Awobokun v The Sketch Publishing Co Ltd & ors*,¹⁸⁶⁵ it was held that the defendants had, by the exclusion of the plaintiff from their meetings in which they considered allegations against him, and also their failure to give him a copy of the report and their recommendation, acted in breach of the rules of natural justice.

Although this case was decided on the basis of the principle of natural justice, the basis of the judgement in the case affirm the fair information principle of allowing individual access to information¹⁸⁶⁶ regarding them, especially when it might result in an unfavourable judgement.¹⁸⁶⁷

7.2.1.2a Relevance to Internet cafes

As mentioned above, Section 39 (3) lends authority to the use of the English Common law confidentiality principles for the protection of privacy. This provision also

¹⁸⁶⁵ (1973) 3 UILR 502.

¹⁸⁶⁶ Cf Buys op cit 379. See Part II of the United Kingdom Data Protection Act Cap 29 of 1998. See specifically section 7(1)(a), (b), & (d).

¹⁸⁶⁷ Ibid. Cf Sections 7(1)(d) & 14 of the United Kingdom Data Protection Act.

encourages the enactment of laws for the protection of data. In essence, there will be constitutional backing for a data protection Act or an Act to provide data in Internet cafes.

7.2.2 Statutory Protection

7.2.2.1 Statutory Protection of Privacy in Nigeria

Apart from the constitutional guarantee of privacy,¹⁸⁶⁸ there is no general statute or body of law formulated for the protection of the right to privacy in Nigeria. However, there are certain statutes that provide limited protection for the right to privacy. These are: the Criminal Code Act,¹⁸⁶⁹ the Penal Code,¹⁸⁷⁰ the Criminal Procedure Act,¹⁸⁷¹ the Evidence Act,¹⁸⁷² the Defamatory and Offensive Publications Act,¹⁸⁷³ the Copyright Act,¹⁸⁷⁴ and the Sharia Penal Code Law.¹⁸⁷⁵ The relevant parts of these Acts will be examined below.

¹⁸⁶⁸ Section 37, LFN 1999.

¹⁸⁶⁹ Cap 77 LFN 1990.

¹⁸⁷⁰ Cap 345 LFN 1990.

¹⁸⁷¹ No 51 of 1977.

¹⁸⁷² Cap 112 LFN.

¹⁸⁷³ Cap 93 LFN 1990.

¹⁸⁷⁴ Cap 68 LFN 1990.

¹⁸⁷⁵ Zamfara State of Nigeria Law No 10, 2000.

7.2.2.1.1 The Criminal Code Act¹⁸⁷⁶

The Criminal Code Act is applicable in the Southern part of Nigeria. The Act generally contains definitions of offences, their punishments and related matters. The Act does not contain specific legislation on protection of privacy but certain of its provisions are relevant. Chapter 17 of the Act provides for offences relating to Posts and Telecommunications. This section contains provisions on the interception of mail, as well as the unlawful keeping or destruction of postal matter and telegrams.¹⁸⁷⁷ Under the Act, it is an offence to intercept mail with the intent to search or steal postal matter.¹⁸⁷⁸ It is also an offence to unlawfully secrete or destroy postal matter or telegrams.¹⁸⁷⁹ These provisions provide limited protection for privacy by prohibiting unlawful interference with, thus ensuring the secrecy of, postal matter and telegrams.¹⁸⁸⁰

7.2.2.1.1a Relevance to Internet Cafes

Although the provisions of Section 17 on posts and Telecommunications does not specifically mention e-mail, it is submitted that as in the case of Germany,¹⁸⁸¹ a broad interpretation should be applied to “telecommunication” and e-mail should be included

¹⁸⁷⁶ Cap 77 LFN 1990.

¹⁸⁷⁷ Sections 161ff.

¹⁸⁷⁸ Section 161.

¹⁸⁷⁹ Section 162.

¹⁸⁸⁰ Cf Article 10 of the German basic Law.

¹⁸⁸¹ Cf above Para 5.1.1.2.

within its purview. Thus, the provisions prohibiting the interception, unlawful keeping and the destruction of postal matter and telegrams will be applicable to e-mail as well as telephonic communication in Internet cafes.

7.2.2.1.2 The Penal Code¹⁸⁸²

The Penal Code is the counterpart of the Criminal Code and it is modelled after the Q'ran (Islamic law).¹⁸⁸³ It is applicable in the Northern part of Nigeria. The provisions of the Penal Code on defamation are, for our purpose, most closely related to the protection of privacy. The Penal Code contains detailed provisions on defamation.¹⁸⁸⁴ In the Penal Code, defamation is defined as words, signs or mechanically produced representations that cause harm to the reputation of another.¹⁸⁸⁵ The Penal Code may be used to protect the right to privacy where an invasion of privacy involves the use of words, signs or mechanically produced representations that cause harm to a person's reputation.

7.2.2.1.2a Relevance to Internet Cafes

Where an Internet café related invasion of privacy involves the use of words, signs or mechanically produced marks to cause harm to the complainant's reputation, there will

¹⁸⁸² Penal Code (Northern States) Federal Provisions Act Cap 345 LFN 1990.

¹⁸⁸³ S Richardson *Notes on the Penal Code Law (Cap 89 Laws of Northern Nigeria, 1963)* (1987) at 1.

¹⁸⁸⁴ Sections 391-393.

¹⁸⁸⁵ Section 391.

be liability under this Act. Thus, where, for instance, a poster or letter containing defamatory words or pictures is produced in an Internet café, using Internet café equipment or by Internet café personnel or third parties, there will be liability for defamation for such publication.

7.2.2.1.3 The Criminal Procedure Act¹⁸⁸⁶

The Criminal Procedure Act prescribes and regulates the procedure to be observed in criminal proceedings. With regard to the description of persons, the Criminal Procedure Act provides that where it is necessary to refer to any person in a complaint, summons, warrant of description or any other document issued by a court in the exercise of its criminal jurisdiction, the description or designation of that person shall be such as is reasonably sufficient to identify him without necessarily giving personal details such as correct name, abode, style, degree and the like.¹⁸⁸⁷ In this way, the privacy of such persons is protected. The Criminal Procedure Act also provides for the protection of information or data such as finger-prints and palm-prints by virtue of Sections.

7.2.2.1.3a Relevance to Internet Cafes

This Act will only be relevant for the protection of privacy in Internet cafes where information protected pursuant to any of the sections in the Act is processed or disclosed

¹⁸⁸⁶ Cap 80 LFN 1990.

¹⁸⁸⁷ Section 147.

through an Internet café. Thus where, for instance, personal information regarding the description of persons in criminal proceedings is published in an Internet café such that personal identifying details are disclosed, there will be liability for such publication.

7.2.2.1.4 The Evidence Act¹⁸⁸⁸

The Evidence Act prescribes the rules regulating the giving of evidence in judicial proceedings. The Act protects the privacy of communications made between husband and wife during their marriage by providing that a husband or wife may not be compelled to disclose such information.¹⁸⁸⁹ Section 164 provides for circumstances under which such information may be disclosed which include the consent of the other party.

Sections 165-176 of the Act provide for official and privileged communications. Under this section, certain categories of information are protected as privileged. Examples of these are, information given to public officials in official confidence;¹⁸⁹⁰ information in the knowledge of magistrates, police officers and officials of the public revenue department, regarding the commission of offences;¹⁸⁹¹ and information given to a legal practitioner by his client professionally.¹⁸⁹²

¹⁸⁸⁸ Cap 112 LFN 1990.

¹⁸⁸⁹ Section 161 (3). Cf Section 198 of the (South African) Criminal Procedure Act 51 of 1977 (as amended) above at Para 7.1.2.1.5 and Section 10 of the South African Civil Proceedings Evidence Act No 25 of 1965 as amended- above Para 7.1.2.1.6.

¹⁸⁹⁰ Section 168.

¹⁸⁹¹ Section 166.

Section 211 of the Evidence Act also provides some protection for the prosecutrix in cases of rape, attempted rape and indecent assault. The provision states that in the cross-examination of the prosecutrix in such cases, she may be asked whether she has had connection with other men but her answer cannot be contradicted. In effect, where the prosecutrix answers in the negative, she cannot be required to give further information on that issue.¹⁸⁹³ In this case, it means the prosecutrix can keep as private, information relating to her relationships with other men and details about her sex life that do not relate to the accused.¹⁸⁹⁴

7.2.2.1.4a Relevance to Internet Cafes

Where information relating to communications between husband and wife that are protected under the Evidence Act is contained in Internet café depositories, there will be privacy protection available for such information. Similarly, where information relating to protected aspects of the life of a prosecutrix in a rape case are contained in Internet café depositories, there will be privacy protection under the Evidence Act in respect of such information.

7.2.2.1.5 The Defamatory and Offensive Publications Act¹⁸⁹⁵

¹⁸⁹² Section 170.

¹⁸⁹³ *R v Holmes* (1871) L.R. ICCR 334. Cf Aguda: *The Law of Evidence* (1989) at 322.

¹⁸⁹⁴ Cf Section 3 of the (South African) Natal Law to amend the Law of Evidence, No5, 1870. Cf above Para 7.1.2.1.7.

¹⁸⁹⁵ Cap 93 Laws of the Federation of Nigeria 1990.

Under the Defamatory and Offensive Publications Act, it is an offence to publish, display or offer to the public any pictorial representation of any person, living or dead, in a manner likely to provoke any section of the community.¹⁸⁹⁶ The Act indirectly protects the privacy of individuals where publication of information may provoke members of the society.

7.2.2.1.5a Relevance to Internet Cafes

The protection for privacy in Internet cafes provided in this Act is somewhat similar to that provided for in the Penal Code.¹⁸⁹⁷ The Defamatory and Offensive Publications Act will be useful for the protection of electronic mail privacy where offensive material is published about a person via e-mail or the Internet in an Internet cafe.

7.2.2.1.6 The Copyright Act¹⁸⁹⁸

Under the Copyright Act, there is some protection for the right to privacy in cases where the invasion of privacy involves the infringement of information stored in permanent form like literary works, musical works and artistic works.¹⁸⁹⁹ Where a person invades the privacy of another by unlawfully publishing or otherwise disclosing the contents of

¹⁸⁹⁶ Section 2(1).

¹⁸⁹⁷ Penal Code (Northern States) Federal Provisions Act Cap 345 LFN 1990.

¹⁸⁹⁸ Cap 68 LFN 1990.

¹⁸⁹⁹ Section 1(1) Copyright Act.

letters, poems or, other literary or artistic works¹⁹⁰⁰ that are copyright protected, or, uses them in any other unlawful manner, such a person will be liable for infringement of copyright.

7.2.2.1.6a Relevance to Internet Cafes

The Copyright Act will provide privacy protection where literary, artistic or musical works processed in an Internet café are subsequently copied without authorisation. Thus, where a poem, song or story sent through Internet café e mail is copied or reproduced without lawful authority, there will be liability for the misuse of this information under the Nigerian Copyright Act.

7.2.2.1.7 The Sharia Penal Code Law¹⁹⁰¹

The Sharia Penal Code Law is applicable in the Zamfara state of Nigeria, and some other Northern States¹⁹⁰² and has provisions protecting the right to privacy. Section 369 deals specifically with invasion of privacy.¹⁹⁰³ Invasion of privacy is defined here in terms of

¹⁹⁰⁰ Cf the English case of *Albert v Strange* [1849] 2 De G & Sm 652, 64 Eng Rep 293 Ch., where the defendants copied the plaintiff's etchings and sought to publish them. However, the defendant in this case brought action for breach of trust and based on his property in the etchings. See above Para 3.2.2.1.

¹⁹⁰¹ Zamfara State of Nigeria Law No 10, 2000. This is different from the Penal Code. Although both Laws are based on Sharia Law, the Penal Code is a less strict version of the Sharia and it was generally applicable in Northern Nigeria before the adoption of the Zamfara state laws, which are stricter.

¹⁹⁰² Although there are 16 Northern States viz: Adamawa, Bauchi, Borno, Gombe, Jigawa, Kaduna, Kano, Katsina, Kebbi, Nasarawa, Niger, Plateau, Sokoto, Taraba, Yobe and Zamfara states, the Sharia is not applied in all of them, for instance in Plateau state, which has a large population of Christians.

¹⁹⁰³ It provides :

prying or intrusions. The protection provided for in that section specifically includes letters and secrets. Section 179 on house trespass also offers protection of the right to privacy where a person enters the property of another with intent to commit an offence, intimidate, insult or annoy a person in possession of such property. Property, in respect of the offence of house trespass, is defined as “any structure, whether temporary or permanent, and includes a house, aircraft, motor vehicle, ship, building, place of worship, hut, store or compound completely enclosed by a wall or other structure.”¹⁹⁰⁴

The law also has provisions on using a false property name,¹⁹⁰⁵ exhibition of false light, mark or buoy,¹⁹⁰⁶ and false impersonation.¹⁹⁰⁷ The provisions on the use of false property name, exhibition of false mark and false impersonation protect goodwill and reputation. Like the tort of passing-off, these provisions generally protect commercial interests and may come under Prosser’s categories of appropriation and false light.¹⁹⁰⁸

It must be noted that the Sharia Penal Code Law is, to a large extent, an Islamic moral code, and some of its provisions are themselves invasions of privacy as well as infringements of other Constitutional rights. For instance, the Code prohibits the drinking

“Whoever invades the privacy of any person by prying into his house without lawful justification, to eavesdrop on him, or read his letters or discover his secrets, shall be punished with imprisonment for a term not exceeding one year or with fine or with both.”

¹⁹⁰⁴ Section 180.

¹⁹⁰⁵ Section 262.

¹⁹⁰⁶ Section 362.

¹⁹⁰⁷ Section 348.

¹⁹⁰⁸ See above Para 1.1.

of alcohol,¹⁹⁰⁹ drunkenness in public and private places,¹⁹¹⁰ lesbianism,¹⁹¹¹ and sodomy.¹⁹¹² It contains other provisions that are infringements on the right to privacy and other fundamental rights guaranteed by the Constitution.¹⁹¹³

Section 40 of the Constitution provides that “every person shall be entitled to assemble freely and associate with other persons” and Section 42 provides that a person shall not be subjected either expressly or in the practical application of, any law in force, to disabilities or restrictions to which citizens of Nigeria of other communities, sex, religion or political opinion are not made subject. It is submitted that on the basis of these two Constitutional provisions, gay and lesbian Nigerians have the right to associate together without being discriminated against or punished.

Section 37 of the Nigerian Constitution also guarantees the privacy of Nigerian citizens and their homes. The provisions prohibiting drinking of alcohol, drunkenness, sodomy and lesbianism in the home would therefore be a direct infringement on an individual’s

¹⁹⁰⁹ Section 149.

¹⁹¹⁰ Section 151.

¹⁹¹¹ Sections 134, 135.

¹⁹¹² Sections 130, 131.

¹⁹¹³ For example, the right to freedom of association provided for in section 40 of the 1999 Constitution FRN. Cf the South African case of *National Coalition for Gay and Lesbian Equality & others v Minister of Justice & others* 1998 (6) BCLR 726 (W) at 753- 754, where a law prohibiting the display of sexual affection between men at parties was declared invalid and inconsistent with Section 8 of the Interim Constitution which prohibited discrimination (at 753-754). Section 127 of the Zamfara state Penal Code which provides for the stoning to death or caning of an adulteress is also an affront to the Constitutional right to life in Section 33 and the right to dignity in Section 34.

Constitutional right to privacy.¹⁹¹⁴ It is submitted in this regard that while Section 369 of the Sharia Code protects the right to privacy of correspondence, the provisions of Sections 149, 151, 130 and of the Sharia Penal Code Law constitute an infringement on other aspects of the right to privacy, as well as other Constitutional rights. The above Sharia Code provisions may thus be challenged as unconstitutional, and on the basis of Constitutional supremacy¹⁹¹⁵ be declared void.

7.2.2.1.7a Relevance to Internet Cafes

The privacy protection provided for in Section 369 of the Sharia Code is qualified by the phrase prying into the house is expressly confined to acts committed in the home. It is therefore doubtful whether this provision will protect information processed in Internet cafes. The provisions relating to the use of a false property name,¹⁹¹⁶ exhibition of false light, mark or buoy,¹⁹¹⁷ and false impersonation¹⁹¹⁸ may however be relevant for the protection of information processed in Internet cafes. Thus, where information so processed constitutes

¹⁹¹⁴ Cf Didcott J in *Case & another v Minister of Safety and Security & others* 1996 (3) SA 617 (CC), 1996 (5) BCLR 609 (CC) where he states as follows: “ what erotic material I may choose to keep within the privacy of my home, and only for my personal use there, is nobody’s business but mine. It is certainly not the business of society or the State. Any ban imposed on my possession of such material for that solitary purpose invades the personal privacy which ... the ... Constitution ... guarantees that I shall enjoy.” (At para 91).

¹⁹¹⁵ Cf the Preamble to the 1999 Constitution.

¹⁹¹⁶ Section 262.

¹⁹¹⁷ Section 362.

¹⁹¹⁸ Section 348.

7.2.2.2 Statutory Protection of Data in Nigeria

There is no Data Protection statute in Nigeria. However, protection of data may be found in the provisions of some statutes like the Computer Security and Critical Information Infrastructure Protection Bill,¹⁹¹⁹ the Nigerian Communications Act,¹⁹²⁰ Wireless Telegraphy Act,¹⁹²¹ and the National Population Commission Act.¹⁹²² There is also a Nigerian Income Tax (Authorised Communications) Act¹⁹²³ which regulates the obtaining and disclosure of tax-related information by government officials.

7.2.2.2.1 The Computer Security and Critical Information Infrastructure Protection Bill¹⁹²⁴

The aim of the Bill is to protect computer systems and networks in Nigeria and to safeguard critical information infrastructure by providing criminal liabilities and penalties for objectionable acts carried out using computers and other information and communication technology devices.¹⁹²⁵ It is applicable to Internet Service providers, Communication Service providers as well as Application Service providers.¹⁹²⁶

¹⁹¹⁹ 2005.

¹⁹²⁰ No 7 of 2003.

¹⁹²¹ 1990.

¹⁹²² Cap 270 LFN 1990.

¹⁹²³ Cap 175 LFN 1990.

¹⁹²⁴ 2005.

The Bill contains provisions prohibiting unlawful access to computers,¹⁹²⁷ unauthorised disclosure of access codes,¹⁹²⁸ fraudulent electronic mail messages,¹⁹²⁹ data forgery,¹⁹³⁰ computer fraud,¹⁹³¹ system interference,¹⁹³² misuse of devices,¹⁹³³ identity theft and

¹⁹²⁵ See the explanatory Memorandum to the Bill.

¹⁹²⁶ Cf Section 34.

¹⁹²⁷ Section 2(1) which provides: “Any person who without authority or in excess of his authority –

- (a) accesses any computer; or
- (b) accesses any computer for the purposes of -
 - (i) securing access to any program or data held in any computer, or
 - (ii) committing any act which constitutes an offence under any enactment or law for the time being in force in Nigeria,
 commits an offence and shall be liable on conviction.”

¹⁹²⁸ Section 3(1) which provides: “ Any person who, knowingly and without authority or in excess of authority, discloses any password, access code or any other means of gaining access to any program or data or database held in any computer for any unlawful purpose or gain, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or to imprisonment for a term of not less than 3 years or to both such fine and imprisonment, and in the case of a second or subsequent conviction, to a fine not exceeding N1,000,000 or to imprisonment for a term of not less than 5 years or to both such fine and imprisonment.”

¹⁹²⁹ Section 4(1): “Any person who with intent to defraud sends electronic mail message to a recipient, where such electronic mail 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 a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment.”

¹⁹³⁰ Section 5: “Any person who knowingly accesses any computer and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data be considered or acted upon as if it were authentic or genuine, whether or not such data is readable or intelligible, commits an offence and shall be liable on conviction to a fine of not less than N500, 000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.”

¹⁹³¹ Section 6: “Any person who knowingly and without right causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer for the purpose of conferring any benefits whether for himself or another person, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.”

¹⁹³² Section 7(1) which provides: “ Any person who without authority or in excess of authority interferes with any computer network in such a manner as to cause any data or program or software held in any computer within the network to be modified, damaged, suppressed, destroyed, deteriorated or otherwise rendered ineffective, commits an offence and shall be liable on conviction to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment.”

¹⁹³³ Section 8: “Any person who unlawfully produces, adapts or procures for use, distributes, offers for sale, possesses or uses any devices, including a computer program or a component or performs any of those acts

impersonation¹⁹³⁴ and unlawful interception,¹⁹³⁵ among other provisions. It also contains provisions on records retention and data protection.¹⁹³⁶ The proposed Act further provides that persons exercising any function under Section 11¹⁹³⁷ should have due regard to the constitutional right to privacy and they should take appropriate technological and organisational measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.¹⁹³⁸ The proposed Act does not provide for any administrative officer to supervise or oversee its operation. It however provides that the President (of the Federal Republic of Nigeria) may prescribe standards, guidelines, rules, procedures for the general management of Critical Information Infrastructure.¹⁹³⁹

relating to a password, access code or any other similar kind of data, which is designed primarily to overcome security measures with the intent that the devices be utilised for the purpose of violating any provision of this Act commits an offence and is liable to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment.”

¹⁹³⁴ Section 10 which provides: “Any person who, with the intent to deceive or defraud, accesses any computer or network and uses or assumes the identity of another person, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.”

¹⁹³⁵ Section 12(1): “Any person who intentionally, without authority or in excess of authority, intercepts any communication originated, terminated or directed from, at or to any equipment, facilities or services in Nigeria commits an offence and shall be liable on conviction to a fine of not less than =N=5,000,000 or to imprisonment for a term of not less than 10 years or to both such fine and imprisonment.”

¹⁹³⁶ Section 11(4) which provides: “ Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act or pursuant to any regulation under this section, shall not be utilized except for legitimate purposes. Under this Act, utilization of the data retained, processed or retrieved shall constitute legitimate purpose only with the consent of individuals to whom the data applies or if authorized by a court of competent jurisdiction or other lawful authority.”

¹⁹³⁷ This section relates to Service providers (Section 34; cf above) and provides for records retention and data protection.

¹⁹³⁸ Section 11(5).

¹⁹³⁹ Part II Section 19.

The Computer Security and Critical Information Infrastructure Protection Bill has however received several criticisms relating to various aspects of the Bill, including the provisions regulating its supervision, administration and enforcement. Firstly, it has been noted that the Bill does not contain any provisions constituting internal or external checks and balances¹⁹⁴⁰ with regard to actions taken by officers pursuant to the Bill. Furthermore, it has been observed that the Bill does not make clear or definite provision for procedure to be followed by law enforcement agencies for the carrying out wiretaps or intercepting communications.

It is submitted that given Nigeria's history of dictatorial leadership,¹⁹⁴¹ any legislation that neglects to specify the powers, limitations of, including specific procedure to be complied with by, any authorities or officers performing duties pursuant to that Act, or legislation that fails to provide a mechanism for accountability of officers acting pursuant to its may become a tyrannical law.

Very significantly, it has also been pointed out¹⁹⁴² that the Bill does not clearly specify the law enforcement agencies responsible for carrying out the provisions of the Bill nor does it provide for any independent officer to monitor or supervise the administration or enforcement of the Bill. Other aspects of the Bill that have received criticism include the failure to provide clear definition of certain key terminology, failure to provide for the

¹⁹⁴⁰ E.O. Oserogho "New Wire Tapping, Cyber Crimes & Anti-Terrorism Bill In Nigeria" *Legalbrief Africa* at <http://www.legalbrief.co.za/article.php?story=20061013091452442> (October 2006) Accessed May 2007.

¹⁹⁴¹ Cf above Para 1.6.

¹⁹⁴² Cf Oserogho "New Wire Tapping, Cyber Crimes & Anti-Terrorism Bill In Nigeria" op cit.

award of compensation for breaches of civil liberties and inadequate provisions regarding other procedural, regulatory and enforcement-related matters.¹⁹⁴³

It is trite that effective enforcement of any law is central to the enjoyment of any rights guaranteed under such law. It is therefore submitted that the shortcomings highlighted above, especially issues surrounding the administration, enforcement and proper procedure of the Bill are critical and must be resolved in order to enjoy the benefits sought to be provided by the proposed Act.

7.2.2.2.1a Relevance to Internet Cafes

The Computer Security and Critical Information Infrastructure Protection Bill contains many provisions that uphold the OECD and EU data protection principles and will be relevant for the protection of information processed in Internet cafes. For instance, the provisions relating to unlawful access to information, unauthorised disclosure, data retention and data protection may be relied on for protection where information processed in an Internet café is accessed unlawfully, disclosed without authority, or retained for an illegitimate purpose.

The provisions requiring the adoption of appropriate technological and organisational measures to safeguard the confidentiality of data are also relevant and in line with one of the principles of data processing. However, since the Act is yet to come into operation

¹⁹⁴³ Ibid.

and considering its shortcomings as highlighted above, the actual nature and extent of (privacy and) data protection afforded by the Act is questionable and remains to be seen upon the completion, coming into effect and application of the Act.

7.2.2.2.2 The Nigerian Communications Act¹⁹⁴⁴

The Act contains broad provisions for the regulation of the Nigerian communications industry. It focuses on administrative and supervisory matters and provides a broad framework for the progress and development of the Nigerian communications industry.¹⁹⁴⁵ The Act does not specifically contain provisions for the protection of privacy. However, Section 64 of the Act contains provisions on the information gathering powers of the Commission for investigative and other administrative purposes. It provides for the production of evidence or information relevant for the use of the Commission in specified circumstances. The Act also requires that any person providing information pursuant to its provisions shall ensure the truth, accuracy and completeness of such information.¹⁹⁴⁶

7.2.2.2.2a Relevance to Internet Cafes

¹⁹⁴⁴ No 7 of 2003.

¹⁹⁴⁵ Cf the Preamble to the Act. See also Section 1.

¹⁹⁴⁶ Section 64(4).

Although the Commission may, in the exercise of its functions,¹⁹⁴⁷ enact laws or policies affecting practice and procedure in Internet cafes, the Act does not contain any provisions that are directly relevant for the protection of privacy in Internet cafes. However, the requirement in Section 64(4) of the Act for truth, accuracy and completeness with regard to information provided pursuant to the Act are noteworthy as they reflect some of the universal data protection principles earlier discussed.¹⁹⁴⁸

7.2.2.2.3 The Wireless Telegraphy Act¹⁹⁴⁹

The Wireless Telegraphy Act prohibits the unauthorised use of wireless telegraphy equipment for the purpose of obtaining information relating to the contents, sender or addressee of any message.¹⁹⁵⁰ The Act also prohibits the disclosure of information relating to the contents, sender or addressee of any message where such information would not have come to the knowledge of the person disclosing it but for the use of wireless telegraphy by such a person or another person.¹⁹⁵¹

7.2.2.2.3a Relevance to Internet Cafes

¹⁹⁴⁷ Cf the Preamble and Section 1 of the Act.

¹⁹⁴⁸ Cf Para 3.

¹⁹⁴⁹ 1990.

¹⁹⁵⁰ Section 39 (1) i.

¹⁹⁵¹ Section 39 (1) ii.

This Act may be relevant for the protection of information processed in Internet cafes where information regarding the contents, sender or addressee of an e-mail message processed in an Internet café is accessed or disclosed via any wireless telegraphy equipment such as a camera.

7.2.2.2.4 The National Population Commission Act¹⁹⁵²

Under this Act, the National Population Commission is empowered to collect information about people in the performance of its lawful duty.¹⁹⁵³ However, the Act also prohibits unlawful disclosure of information. Section 19(1) prohibits unlawful publication or communication of information obtained in the course of duty by a person employed for the purposes of the Act, and prescribes a punishment of a fine or imprisonment. Section 19(2) prohibits publication or communication of information¹⁹⁵⁴ by any person who knows that the information has been disclosed in contravention of the Act.

7.2.2.2.4a Relevance to Internet Cafes

This Act will only be relevant for the protection of data where any information protected under the Act is published through an Internet café.

7.2.3 Conclusion on Statutory Protection of Privacy and Data in Nigeria

¹⁹⁵² Cap 270 LFN 1990.

¹⁹⁵³ See part V; See also Section 24 in the Third Schedule (Part I) of the Constitution of the Federal Republic of Nigeria 1999.

¹⁹⁵⁴ Section 19.

In Nigeria, the Constitution contains a general provision for the protection of privacy, which, if interpreted and applied would afford basic privacy protection. Statutory provisions protecting privacy also afford limited protection within the scope of the subject matter to which they relate. As for data, the Constitution does not make sufficiently direct or detailed provisions for its protection¹⁹⁵⁵ and the available statute law is significantly limited in scope.

Although, the Computer Security and Critical Information Infrastructure Protection Bill contains several provisions for the protection of computer processed information, it yet to be enacted into law and cannot as yet be relied on for protection. Therefore, extremely limited privacy and/or data protection may be found in other statutes.¹⁹⁵⁶

In sum, while the Constitution provides a suitable basis for the protection of privacy in Nigeria, constitutional protection of privacy has not been maximally explored in Nigeria. Other available laws on the protection of privacy and data in Nigeria are few and the protection afforded in these provisions are also limited. In essence, for practical purposes, there is only limited privacy and data protection available in Nigeria.

7.3 Conclusion on the Law Protecting Privacy and Data in South Africa and Nigeria.

¹⁹⁵⁵ Section 39(3); Cf above Para 5.2.1.2.

¹⁹⁵⁶ Above Para 5.2.2.2.

It is clear from the above analysis that although statutory protection of the right to privacy is limited in South Africa, the Constitution provides effective protection for the right to privacy. With respect to data, although there is no data protection law, other constructive laws protecting information are available. For instance, the Statistics Act provides detailed protection for information that qualifies as 'statistics' under the Act and the provisions of the Promotion of Access to Information Act as well as certain other Acts make limited provision for the protection of privacy and data. Nonetheless, none of these statutes protects information or data in general and their provisions are not sufficiently comprehensive in this regard.

In Nigeria, while protection is provided for the right to privacy in the Constitution and under certain statutes, there is very little constitutional or statutory protection for data. As in South Africa, there are certain statutes which contain useful privacy and data protection provisions but these are limited. There is a clear need to develop the law of privacy in Nigeria on the basis of the Constitution. In this regard, the Nigerian courts are encouraged to consider the early English Common Law cases, cases decided on the basis of the Human Rights Act¹⁹⁵⁷ as well as the cases of Constitutional invasions of privacy in South Africa and the United States, as being of persuasive value in developing a Constitutional right to privacy in Nigeria. There is also a need to enact data protection legislation.

¹⁹⁵⁷ Chapter 42 of 1998. Cf above Para 3.2.2.1.1.

7.3a Relevance to Internet Cafes

The conclusions reached above are applicable to the Internet cafes. For instance, in South Africa, the Constitutional guarantee of privacy provides a basis for the protection of information processed in Internet cafes while certain other statutes also contain relevant provisions in this regard. The available data protection in South Africa is limited to what is obtainable under the different statutes. In Nigeria, the protection available for information processed in Internet cafes is limited in terms of the constitutional provisions and the few available statutes. As for data protection, this is virtually nonexistent apart from the protection available by means of Section 36 of the Constitution, the sparse provisions in other statutes and the provisions of the Computer Security and Critical Information Protection Bill.

In the light of the foregoing analysis of Common Law and the statutory protection of privacy and data in South Africa and Nigeria, and the preceding examination of the protection of privacy and data in the United Kingdom, the United States and Germany, suggestions will now be made for reform of data protection law in Nigeria.

CHAPTER EIGHT

SUGGESTIONS FOR REFORM OF PRIVACY AND DATA PROTECTION LAW IN NIGERIA

8.1 Suggestions for the Reform of Privacy Law in Nigeria

From the above analysis of Nigerian privacy and data laws, the following options are available for development. The first is the development and adaptation of the Nigerian Common Law through the resourceful and unrestrictive application of available Common Law principles. In this regard, specific principles and ideas from other legal systems highlighted above may be consulted for guidance. These include, the adoption of the English Common law breach of confidence principles.¹⁹⁵⁸ Prosser's categorisation of torts¹⁹⁵⁹ may also be adopted loosely in Nigeria to guide the courts in identifying and grouping the available privacy interests.

Further to this, it is suggested that as in South Africa,¹⁹⁶⁰ the principles of the Constitution be utilised to shape the common law. This will be applicable, for instance in the determination of the prevailing *boni mores*. It is however submitted that adaptation of the Common Law alone will not bring about the required development of the law of privacy in Nigeria for the following reasons:

¹⁹⁵⁸ Cf above Para 3.2.2.1.1.3.

¹⁹⁵⁹ Cf above Para 1.1.

Firstly, unlike statute law, which can be made to address both immediate and future situations, the Common Law develops very slowly,¹⁹⁶¹ on a case-by-case basis. Furthermore, judges are bound to follow precedents unless they can distinguish between the facts of previous cases and the one before them. Change is therefore very slow in the Common Law system,¹⁹⁶² and case law is not the most suitable instrument for law reform, especially where the need for change is long overdue. This is not to discount the value of measured legal development on a case by case basis,¹⁹⁶³ but to suggest additional measures to increase their effectiveness for our purpose.

In this regard, a second suggestion for the development of Nigerian privacy law is the development of Section 37 of the Nigerian Constitution. In this regard, it is suggested that Section 37 be interpreted broadly, like the guarantee of the “right to respect for private and family life, home and correspondence” provided for in the Human Rights Act,¹⁹⁶⁴ to offer protection in respect of both substantive and informational privacy rights.¹⁹⁶⁵ It is further suggested that cases decided in the United Kingdom based on the recognition of the right to privacy in the Human Rights Act be relied on as persuasive authority.

¹⁹⁶⁰ Cf above Para 7.1.1.

¹⁹⁶¹ Cf Roos op cit at 718 in her conclusion on South African data protection law.

¹⁹⁶² Cf English Common Law development of the right to privacy- above Para 3.2.2. See particularly Para 3.2.2.1.2.

¹⁹⁶³ Cf the development of the South African privacy law on the basis of the Constitution and the Common law. See above Paras 6.1.1 & 7.1.1.

¹⁹⁶⁴ Cap 42 of 1998 Article 8.

¹⁹⁶⁵ Cf above Para 3.2.3.1.1.

Further to this, it is suggested that Section 37 of the Nigerian Constitution should be read together with Section 34 of the Constitution, which guarantees the right to dignity of the human person, and these provisions should be interpreted broadly as in Germany.¹⁹⁶⁶ (In this regard, it must be mentioned that the South African courts also consider dignity as an aspect of privacy.)¹⁹⁶⁷ It is submitted that the juxtaposition of these provisions will provide a firmer and broader foundation for the protection of different types of privacy invasions.¹⁹⁶⁸ Such flexibility will be conducive for the growth and development required in this aspect of the law in Nigeria.

It must be said that the constitutional guarantee of privacy will be limited in terms of Section 45 of the Constitution which permits the making of laws that are “reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health or for the purpose of protecting the rights and freedoms of other persons.”¹⁹⁶⁹ In essence, where any law would constitute an infringement of the provisions of the Constitution, such law would be valid if it is enacted in the interest of defence, public safety, public order, or public morality- provided that such law can be shown to be reasonably justifiable in a democratic society.¹⁹⁷⁰

¹⁹⁶⁶ Cf 1 *BverfGE* 27 (1969) Cf above Para 5.1.

¹⁹⁶⁷ See the Constitutional Court in *National Coalition for Gay and Lesbian Equality & others v Minister of Justice & others* 1998 (6) BCLR 726 (W); 1998 (2) SACR 102 (W).

¹⁹⁶⁸ *Ibid.*

¹⁹⁶⁹ Section 45 (1) a & b. Cf Section 36 of the South African Constitution Act 108 of 1996.

¹⁹⁷⁰ Cf Section 36 of the South African Constitution Act 108 of 1996.

It is submitted that the inclusion of public morality among the factors that may limit the enjoyment of constitutionally guaranteed rights raises some concern because public morality is a shifting and flexible concept, and is differently perceived from culture to culture. For instance, the Sharia law, which is an Islamic moral code, is acceptable only in certain parts of Northern Nigeria.¹⁹⁷¹ It might thus be challenging to accurately or fairly determine a common morally acceptable standard. It must be borne in mind in this regard that the denial of a person's rights on the basis of other people's sense or standard of morality may constitute injustice or inequality to certain disadvantaged minority groups.¹⁹⁷²

8.1a Relevance to Internet Cafes

The general development of the right to privacy by any of the means suggested above will be of benefit for the protection of privacy in Internet cafes in that such development will ultimately provide a solid foundation for Internet café privacy and data protection. In addition to this general benefit, it has been shown¹⁹⁷³ in particular that the application of the principle of confidentiality¹⁹⁷⁴ and the adoption of the wide interpretation given the

¹⁹⁷¹ Cf above Para 7.2.2.17.

¹⁹⁷² Cf the South African case of *National Coalition for Gay and Lesbian Equality & others v Minister of Justice & others* supra.

¹⁹⁷³ Above Chapter 3.

¹⁹⁷⁴ See Para 3.2.2.1.1ff.

relevant provisions of the Human Rights Act¹⁹⁷⁵ will be beneficial for the protection of privacy in Internet cafes.

8.2 Suggestions for the Reform of Data Protection Law in Nigeria

Regarding data protection in Nigeria, the Constitution recognises the need for the protection of data but does not contain any direct provisions protecting data. As is the case with the protection of privacy, limited protection can be found for data under different statutes dealing with specific areas of information. In the Common Law of Nigeria, there is very limited protection of data, thus the need for a comprehensive Data Protection Act in Nigeria.

As for data protection, considering that there is no Nigerian data protection Act, that the available statutory provisions protecting data are extremely limited and that the only available legislation that purportedly affords fairly broad data protection is contained in a Bill,¹⁹⁷⁶ yet to come into effect and is presently significantly flawed,¹⁹⁷⁷ there remains a definite need for legislation protecting data generally and in particular information processed in Internet cafes in Nigeria. In this regard, it is suggested that the OECD Data Protection principles/ EU Fair Information principles¹⁹⁷⁸ adopted in the United

¹⁹⁷⁵ See Para 3.2.3.1.1 ff.

¹⁹⁷⁶ The Computer Security and Critical Information Infrastructure Protection Bill 2005.

¹⁹⁷⁷ Cf above Para 7.2.2.2.1.

¹⁹⁷⁸ Cf above Para 3.2.3.2.1.2.

Kingdom¹⁹⁷⁹ and Germany¹⁹⁸⁰ and reflected in the proposed South African data Act¹⁹⁸¹ should also be adopted/ reflected in the Nigerian Data Act. This will ensure a high level of data protection in Nigeria both generally and for information processed in Internet cafes.

Regarding the Computer Security and Critical Information Protection Bill¹⁹⁸² which contains relevant data protection provisions, it is proposed that the suggestions given in this work be considered and incorporated into the final Act.

As for the model of protection to adopt, the most suitable and workable model for the protection of privacy and data, taking into consideration all the relevant factors in the country, including technology and the socio-cultural milieu, availability of resources in the country, should be adopted. Nigeria is a developing, multi-cultural federation of thirty-six states consisting of people of about 120 million people of different cultures and languages. It is submitted that, a Privacy and Data Protection Act that can be enforced at the central or federal, as well as the state level may be better suited to Nigeria as it may be more effective to administer the Act at the state level than it will be for a single official to administer the Act to such a population.

¹⁹⁷⁹ Cf above Para 3.2.3.2.

¹⁹⁸⁰ Cf above Para 5.3.2.

¹⁹⁸¹ Cf above Para 7.1.2.2.

¹⁹⁸² 2005.

Furthermore, like Germany, Nigeria is a federation having laws that operate at the federal and state levels, and in some cases, different laws between states. For example, at present, the Criminal Code¹⁹⁸³ is the applicable law in respect of criminal offences in Southern Nigeria, while the Penal Code¹⁹⁸⁴ applies to the Northern part of Nigeria. Furthermore, the Sharia Law is applicable in certain states in Northern Nigeria. In effect, a dual system of law is already in place in Nigeria and it is possible to adopt a similar system for data protection. With regard to Internet cafes, it may be beneficial to adopt a dual system of administration in respect of any data protection laws in Nigeria.

It is therefore submitted that a dual system of data protection as in Germany, whereby a designated official enforces and monitors compliance with a comprehensive set of laws at the national level, and other officials administer the laws at the state level may be feasible. The national official will be responsible for public education and international liaison where necessary. The Act will also make provision for persons or bodies to be involved in the administration of the Act and will specify duties and responsibilities in this regard.

8.2a Relevance to Internet Cafes

¹⁹⁸³ Cap 77 LFN 1990.

¹⁹⁸⁴ (Penal Code (Northern States) Federal Provisions Act) Cap 345 Laws of the Federation of Nigeria 1990.

As has been established,¹⁹⁸⁵ the adoption of the OECD and EU Directive principles in any law for the protection of data will be a positive step. Reflection of these principles in any legislation regulating information processed in Internet cafés is thus highly recommended as a constructive and progressive measure. In addition, certain Common Law breach of confidence principles, as well as the Nigerian Constitution have been identified¹⁹⁸⁶ as useful for the purpose of developing Nigerian (privacy and) data protection laws and useful for the protection of information processed in Internet cafes.

In the light of the foregoing analysis, the following principles and provisions to be included in an Act for the protection of privacy and data generally and in Internet cafes in Nigeria will be outlined.

¹⁹⁸⁵ Para 3.2.3.2.2.5b; cf Paras 3.2.3.2; 5. 3.2; 7.1.2.2;

¹⁹⁸⁶ Above Paras 3.2.2.1ff, 7.2.1 and 8.1.

CHAPTER NINE

PRINCIPLES AND PROVISIONS FOR THE PROTECTION OF PRIVACY AND DATA IN NIGERIA

9.1 Purpose

The purpose of the Act will be, on the basis of the constitutional rights to privacy, self-determination and dignity, to provide for the protection of privacy and data with particular reference to information processed in Internet cafes in Nigeria.

9.2 Scope

The proposed Nigerian Privacy and Data Act will apply to:

- (1) Automated and manual processing
- (2) Electronic, sound, image and print transfer
- (3) Natural and juristic persons
- (4) Information processed by both the public and private sector

With regard to automated and manual processing, it is essential to provide for both paper-based and computer-held records, as a large amount of information is still stored in paper files in Nigeria. Internet café owners will also come under the Act by virtue of the fact

that the Act applies to the transfer of print, sound, image as well as electronic transfers. Thirdly, it is important that the Act apply to natural as well as juristic persons so that Internet café owners, whether they are registered as corporations, or not will be included under the purview of the Act. However, the scope of the Act is not so-delimited only for the purpose of information processed in Internet cafes. Rather, it is intended that the Act will be generally applicable to all persons and bodies who process information. Although there are slight differences in wording, these categories are generally covered in the scope of the proposed South African Protection of Personal Information Act.¹⁹⁸⁷

9.3 Liability

Liability under the Act will be for acts amounting to invasions of privacy and acts amounting to data infringement. In this regard, it is suggested that generally, liability be imposed for any act constituting an invasion of privacy under the Constitution as well as for breach of confidence under the Nigerian Common Law. Since the jurisprudence available on the constitutional right to privacy in Nigeria is limited, it is suggested that for guidance, the privacy interests recognised under the South African Common Law be adopted and that the Act specifically enumerate and provide for liability in respect of intrusions, publication of private facts, appropriation, false light.

¹⁹⁸⁷ (2005) See South African Law Reform Commission Issue Paper 24 Project 124 *Privacy and Data Protection* at www.server.law.wits.ac.za/salc/issue/issue.html at Para 1.3.14. (Cf above Para 7.1.2.2.).

Although this approach may result in some overlap in the protection afforded, it is submitted that this will be a positive feature as protection in respect of these categories will then be better guaranteed.

In addition to the general provisions above, it is suggested that the Act contain detailed and specific provisions for the protection of data. This will include definitions of terminology, enumeration of officials, apportionment of rights, duties, procedure and other relevant provisions in respect of which there will be penalties for non-compliance.

Lastly in discussing liability under the Act, particular emphasis must be laid on the definition section as it will play a pivotal role in determining liability by providing guidance as to where to draw the boundaries regarding whether the facts of any given case fall within the purview of the Act. Hence it is essential for the Act to include clear and detailed definitions of basic terminology that will be generally or frequently used in the Act. This will include such terms as confidential information, data, data controller, data subject, Internet café, Internet café personnel, processing, to mention a few.

In addition to proper terminology definition, the Act should clearly enumerate officers contemplated under the Act and unequivocally define their roles. To illustrate the role of terminology definition in determining liability under the Act, an example may be made of the term "processing" which must be sufficiently broad as to cover all forms of present day information usage.¹⁹⁸⁸ Similarly, the definition of data controllers under the Act must

allow for the inclusion of Internet café operators. In effect, definitions must be couched to give effect to the general intent, purpose and scope of the Act.

9.4 Principles

From the analysis in the preceding chapters, it is submitted that the following principles should be adopted for the effective protection of data and privacy in Internet cafes in a Nigerian Act. The principles have been derived through analysis of the principles contained in COE Convention,¹⁹⁸⁹ the OECD Guidelines¹⁹⁹⁰ and the European Union Directive-¹⁹⁹¹ as reflected in the United Kingdom Data Protection Act.¹⁹⁹² While the essence of the principles remains unchanged there are slight modifications in the nomenclature of some of the principles. In the light of the interconnected nature of the principles, decidedly related principles have been grouped together to enhance cohesion, consistency and concord in the interpretation and application of the Act in Nigeria.

¹⁹⁸⁸ Cf the definition of “processing” in Part 1 Section 1 of the United Kingdom Data Protection Act Cap 29 of 1998.

¹⁹⁸⁹ Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data - ETS No 108 1981.

¹⁹⁹⁰ Organisation for Economic Cooperation and Development’s Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data 1981.

¹⁹⁹¹ Directive 95/46/EC 1995.

¹⁹⁹² Cap 29 of 1998.

It has also been attempted to locate the relevance of the principles within the context of Internet cafes. Notwithstanding the focus on Internet cafes, it must be stressed that the principles elucidated here will be applicable for general data protection law in Nigeria. Finally, it must be clarified that the following is not intended to be a detailed draft of the principles as they will appear in the proposed Act. It is meant to provide a foundation and framework for the building of comprehensive legislation. Thus general principles, will be highlighted, briefly commented on and where necessary, supported with suggestions as to specific provisions.

(1) First Principle: Fair and Lawful Processing

This principle establishes the condition that processing be just and equitable and in compliance with applicable law.¹⁹⁹³ The requirement for lawfulness will be met if processing is done in accordance with general procedure and standards provided for in the Act. This underlines the need for general standards, guidelines and procedure to be set out in the Act. However, in addition to these general standards, it is suggested that the Act specify requirements to be met in order for the criterion of “fair and lawful processing” to be satisfied.¹⁹⁹⁴

As for the fairness requirement, in line with the natural justice and fairness rule *audi alteram partem*, where information is being or will be processed about a person, the

¹⁹⁹³ Cf above Para 3.2.3.2.2.5a (1).

¹⁹⁹⁴ Ibid.

data subject should be allowed to have a say in the process. To give effect to this, the consent of the data subject should be obtained. Thus it is suggested that the requirement for fair processing will be satisfied if the consent of the data subject is obtained. Obtaining of the data subject's consent is also highlighted in the United Kingdom Data Act¹⁹⁹⁵ as a requirement for fair and lawful processing.

However, in order to make sound decisions as to the giving or refusal of consent, it is necessary for the data subject to be well informed. In this regard, it is suggested that the Act generally promote a policy of transparency regarding practices, policies and developments in respect of personal data. Specifically, it is recommended that the Act include provisions similar to those of the 1998 United Kingdom Data Act¹⁹⁹⁶ specifying practice and procedure to be followed by data controllers in conforming with the openness policy.

This will include among other provisions, provisions specifying practical means by which data subjects may be informed about data collection or processing that may affect them and a requirement that data must be obtained directly from the data subject where practicable. Thus it is suggested that the fairness requirement will be fulfilled where the data controller can be shown to have acted in conformity with the conditions for openness and consent of the data subject has been obtained. It must be clarified that the requirement for consent is only one of the conditions to be met for

¹⁹⁹⁵ (Cap 29 of 1998) Cf Schedule 2 of the DPA. Cf above Para 3.2.3.2.2.5.a (1).

¹⁹⁹⁶ Cf above Para 3.2.3.2.2.5.a (1).

fair and lawful processing. Other grounds of justification¹⁹⁹⁷ exist which, if present, will render processing without the consent of the data subject fair and lawful.

In sum, the First principle, which provides for fair and lawful processing of data consists of three general conditions to be fulfilled viz: openness on the part of the data controller, consent of the data subject and processing in accordance with applicable law. The requirement for fair and lawful processing is also identified by Roos¹⁹⁹⁸ as one of the ten core data protection principles to be given effect to in any data protection legislation. It is the first principle enumerated in the proposed South African data Act.¹⁹⁹⁹ The proposed Act also incorporates the Openness principle.²⁰⁰⁰

Application of this principle to Internet cafes will mean that processing must not constitute a violation of any relevant law and that Internet café operators must notify customers of any relevant information relating to the gathering, collating, or other use of information relating to them (customers). The First principle will also require that customers give their consent, or that other grounds of justification exist, for such processing to be done.

¹⁹⁹⁷ For instance the legitimate needs of a third party or public/state interest. Cf Schedule 3 of the 1998 United Kingdom Data Protection Act above at Para 3.2.3.2.2.5(a)(i). See also below Para 9.5.

¹⁹⁹⁸ At 720, 721. Note that while the requirements for fair and lawful processing, and openness and transparency represent separate aspects of the ten core data protection principles identified by Roos, this work takes a slightly different approach whereby consent and the Openness principles are the key components of the requirement for Fair and Lawful Processing. It must be mentioned that Roos also asserts (Chapter 6 Para 2.2.1, chapter 7 Para 5, chapter 9 Para 3) that the requirement for fair and lawful processing will be met if all the other principles are complied with.

¹⁹⁹⁹ Part A Sections 7-10 of the proposed Protection of Personal Information Act 2005.

²⁰⁰⁰ Part A Section 16.

(2) Second Principle: Purpose Enumeration and Conformity with Purpose

The second principle prescribes that the purpose for which data is being processed must be stated clearly and unequivocally, data must be processed in keeping with the stated purpose, and disposed after the specified purpose has been achieved. It must be noted that there are three different aspects to this principle, each of which must be complied with. By virtue of the Second principle Internet café operators will be required to inform customers of the potential for the accumulation of information on their computer systems and also clearly state any purpose(s) for which they may need to access, transfer, disclose, or otherwise process such information. Any processing of information must then be done within the confines of the stated purpose.

Further to this, Internet café personnel will be required to delete personal information from their computers once the purpose for which it was processed has been served. This principle will be very useful to restrict the arbitrary transfer, exchange or other use of information via the Internet in Internet cafes. It will also restrict the accumulation or retention of information on such publicly used computers thus decreasing the potential for any unlawful use of such information by third parties.

The Purpose Enumeration and Conformity principle reflects the OECD Purpose Specification and Use Limitation principles and is also analogous to the Purpose Specification²⁰⁰¹ and Further Processing Limitation²⁰⁰² principles in the proposed

South African data Act. It also reflects the Purpose Specification and Minimality principles as highlighted by Roos.²⁰⁰³

(3) Third Principle: Data Quality

The data processed must be adequate, relevant and proportional with reference to the purpose specified (for processing). Data must also be accurate and up-to-date. The Data Quality principle provides a standard for the processing of personal information especially with regard to information contained in government data banks or those of other private agencies involved with the collection, collation, analysis, storage or other use of data.

It will also be useful for the protection of information processed in Internet cafés, for example, in cases of intrusion or disclosure where the defendants intentionally accesses or, either intentionally or negligently, publishes information that is irrelevant to the given purpose. The Data Quality principle is included in Roos'²⁰⁰⁴ enumeration of ten core data protection principles. It is also included among the Information protection principles in the proposed South African Data Protection Act.²⁰⁰⁵

²⁰⁰¹ Part A Sections 11-13.

²⁰⁰² Part A Section 14.

²⁰⁰³ Op cit Chapter 6 Paras 2.2.1 and 2.2.2 and at 720; Chapter 6 Para 2.2.3 and at 720.

²⁰⁰⁴ Op cit Chapter 6 Para 2.2.4 and at 720-721.

²⁰⁰⁵ Part A Section 15.

(4) Fourth Principle: Individual Participation

The Individual Participation principle calls for measures to ensure that data subjects are able to personally take action concerning the processing of data relating to themselves. To give effect to this, certain personally enforceable rights must be recognised as accruing to data subjects. These will include the right to access information relating to them, the right to be given reasons for denial of access to such information, the right to rectify, or procure erasure of inaccurate or irrelevant data among others and to prevent certain kinds of processing. The Individual Participation principle is included among the core data protection principles identified by Roos.²⁰⁰⁶ It is also included among the conditions for the lawful processing of personal information in the proposed South African Data Act.²⁰⁰⁷

(5) Fifth Principle: Accountability

This principle flows from the recognition of data subjects' rights. Although data subjects have rights in respect of which they can personally take action, the duty of implementing measures to ensure that these rights are upheld lies with data controllers since the processing is done by them, not primarily for the benefit of the data subject. In this regard, the Act should provide for the duties of data controllers and also provide penalties for their breach. These duties should include timely notification that

²⁰⁰⁶ Op cit Chapter 6 Para 2.2.6 and at 721.

²⁰⁰⁷ Part A Sections 21-22.

information is being processed, and the communication of information to the data subject generally in line with the Openness principle.

Application of the accountability principle may require the establishment of a code of conduct for data controllers.²⁰⁰⁸ This is recommended for Internet café operators. It is suggested that the duties of Internet café operators be set out and incorporated in a code of conduct which will be made available to customers. It is suggested that the Code of Conduct should clearly state that customers in Internet cafes have privacy and data protection rights. The Code of Conduct should further assert that Internet café operators have a duty to ensure that these rights are not violated and it should specifically enumerate the duties of Internet café operators. Customers will thus be armed with general information about their privacy rights as well as the knowledge of specific factors to identify in determining whether those rights have been violated by Internet café operators.

It is further suggested that the code of conduct make explicit reference to the role of the proposed Nigerian Data Act as well as the Constitution in the protection of privacy and data. The Code of conduct will thus serve the dual purpose of enhancing the enforcement of data subjects' rights under the proposed Act and being a vehicle for general enlightenment about the right to privacy in Nigeria.

²⁰⁰⁸ Cf OECD Guidelines Explanatory Memorandum 32.

The principle of accountability is included in the ten core data protection principles enumerated by Roos.²⁰⁰⁹ It is also one of the Information Protection Principles in the proposed South African Protection of Personal Information Act.²⁰¹⁰

(6) Sixth Principle: Confidentiality and Sensitivity

The proposed Nigerian data and privacy Act should contain a general provision imposing a duty of confidentiality on data processors. The duty of confidentiality will stipulate that in all cases, a general duty not to disclose confidential information will be imposed on persons processing data unless the consent of the data subject is obtained. In this regard, it is essential that the Act include a clear definition of “confidential information” and “processing” and that the definitions provided be sufficiently broad.

The Act should contain detailed provisions on the obtaining of consent and also provide for other instances in which breach of a duty of confidence will be justified.²⁰¹¹ It is further suggested that the duty of confidentiality should continue after data controllers are no longer involved in the line of work that brought them into contact with the personal information.²⁰¹²

²⁰⁰⁹ Op cit Chapter 6 Para 2.2.10 and at 721.

²⁰¹⁰ (2005) Part A Section 23.

²⁰¹¹ Cf below Para 9.5.

²⁰¹² Cf the duty of confidentiality under the German Federal Data Act (above Para 5.3.2).

In addition to the general provision imposing a duty of confidentiality, it is suggested that the Act should contain a specific list of information to be classified as “sensitive information”, which data controllers will be prohibited from processing except under specified conditions. Sensitive information will consist of delicate and personal information, which if disclosed, may be used in a manner that will adversely affect the data subject or render the data subject vulnerable.²⁰¹³ This will include personal information relating to race, ethnicity, political and religious affiliation, sexual life, physical or mental condition, offences previously committed and so forth.

It is also essential that the conditions under which processing of sensitive information will be permitted be set out in detail. These will include the general categories of exemptions identified below²⁰¹⁴ as well as other specific provisions.

As for its utility for the protection of information processed in Internet cafes, the confidentiality provision will make all disclosure of confidential information processed in Internet cafes *prima facie* unlawful thus shifting the onus on the Internet café operator or other defendant to prove that there was consent or other justification for such disclosure. Similarly, the provision on sensitive information will render the processing of any information which qualifies as “sensitive” *prima facie* unlawful unless one of the conditions specified in the Act permitting processing can be satisfied.

²⁰¹³ Cf below Para 3.2.3.2.2.5a (1) for details on sensitive data in the United Kingdom Data Protection Act.

²⁰¹⁴ Para 9.5.

The Confidentiality and Sensitivity principle is a reflection of Roos' Sensitivity principle,²⁰¹⁵ and Confidentiality principle (as contained in the Security and Confidentiality principle).²⁰¹⁶ Although the Confidentiality principle is not expressly included among the Fair Information Principles enumerated in the proposed South African data Act, it is directly mentioned in connection with the exemptions to the prohibition on the processing of information relating to health or sexual life.²⁰¹⁷ The requirement for sensitivity is also positively affirmed in the provision prohibiting the processing of Special Personal Information²⁰¹⁸ in the proposed Act.

(7) Seventh Principle: Security Safeguards

The implementation of security measures to safeguard the privacy of information processed is a necessity. As custodians of personal information, data controllers should be impressed with the duty of taking reasonable precautionary technological and organisational measures for the prevention of accidental or unlawful access to, disclosure, alteration, erasure or other use of information for the protection of the persons to whom the information relates.

²⁰¹⁵ Cf Chapter 6 Para 2.2.8, p 721

²⁰¹⁶ Cf Chapter 6 Para 2.2.9, p 721.

²⁰¹⁷ Section 29 (4).

²⁰¹⁸ Part B Section 24.

This proviso does not impose an obligation on data controllers to install the most expensive technological security gadget available. It will be sufficient if a data controller takes reasonable steps and means considering the nature of the information to be protected, the state of the art and the cost of implementation to ensure the safe keeping of information in their custody.

Thus for instance, with regard to manually kept data, it should ordinarily be sufficient if confidential information is clearly marked “confidential” and securely stored in a locked personal filing cabinet in the office. For information processed by automated means, the circumstances of each case will also have to be considered however, for information processed in Internet cafes, it will be expected that at the least, Internet café owners install privacy protection software and updates where they are available and affordable and that they ensure that customers are aware of the importance of, and aided to execute, proper log out after each computer session.

The Security Safeguards principle is included among the ten core data principles identified by Roos.²⁰¹⁹ It also represents one of the Fair information principles enumerated in the proposed South African data Act.²⁰²⁰

9.5 Exemptions

²⁰¹⁹ Chapter 6 Para 2.2.9 and p 721.

²⁰²⁰ Part A Sections 17-20.

There should be a general provision for exemption from the scope of the proposed Act where processing will not pose a threat to privacy or constitute an infringement of data. These will include cases where personal information is processed by individuals for domestic purposes, or where information being processed has been de-identified such that it is not possible to re-identify the individuals to whom they apply and in other circumstances as may be prescribed by the Act.²⁰²¹

Further to this, the principle of balancing of rights²⁰²² will apply with regard to the rights provided for under the proposed Act. Thus these rights may lawfully be abridged or withheld where there is a conflict between them and public interest, state interest or the legitimate rights of another individual. Accordingly, it is suggested that the Act generally provide for exemptions with respect to these enumerated interests.

Further to this, there should be exemption from compliance with principles or procedure set out in the Act, for the protection of the data subject. This may arise where there is an urgent need for access to personal information under circumstances where delay or denial of access occasioned by strict compliance would result in an adverse consequence to the data subject.²⁰²³ It must be mentioned that this is not a closed list; it merely represents

²⁰²¹ Cf Roos op cit at 720 and Chapter 2 Section 4 of the proposed South African Personal Information Act 2005.

²⁰²² Cf above Para 1.1.

²⁰²³ Where for example, by reason of the data subject's illness s/he is incapable of making a sound decision regarding consent for access to medical records that are crucial for the immediate treatment of the data subject.

selected general categories within which instances of non-compliance with specified provisions of the Act relating to standards or procedure may be justified.

9.6 Administration and Enforcement

It is trite that the administration and enforcement of the Data Act will be pivotal to its effectiveness²⁰²⁴ therefore definite and clear provision for this should be made. There should be provision for an independent official whose duty it is to administer and supervise compliance with the Act. If the Act is applied at both the Federal and state levels as previously suggested,²⁰²⁵ adequate provisions should be made for supervising/administering officials at both federal and state levels. The Act should clearly state the title and functions of each officer and also specify their duties and responsibilities.

Furthermore, it is suggested that there should be mechanisms for enforcing compliance with the duties impressed upon officials under the Act and penalties prescribed for non-performance of those duties.

9.7 Conclusion

Although all aspects of any given legislation are significant, certain features are of intrinsic import and ultimately determine the quality of the rights guaranteed in the Act,

²⁰²⁴ Cf the United States Privacy Act above at Paras 4.3.1.1 and 4.4. See also the criticism levelled against the proposed Nigerian Cyber Act above at Para 7.2.2.2.1.

as well as the Act's general effectiveness in achieving its set purpose. The selected aspects of the proposed data Act above have been emphasised with the aim that the elements identified as germane to the effectiveness of the proposed data Act be given appropriate attention, thus increasing its chances of success.

The highlight of this work is however the data protection principles. Having been evolved from international documents, adopted /reflected in the United Kingdom, German and proposed South African, Data Protection Acts among others, recognised and affirmed by veritable legal scholars and shown to be relevant in Nigeria, it may safely be asserted that these principles will provide the expected foundational support for general data protection legislation as well as the protection of information processed in Internet cafes in Nigeria.

²⁰²⁵ Cf Roos op cit at 723-724.

CHAPTER TEN

SUMMATION AND CONCLUSIONS

10.1 Overall Summary

From the above analysis of the privacy and data laws of the United Kingdom, the United States, Germany and South Africa, it emerges that while there is no statute or other body of law enacted for the protection of privacy and data in Internet cafes in any of these countries, there are other laws protecting privacy and data in place. It is also clear that the privacy and data protection laws in each of the countries have developed at different paces.

10.1.1 United Kingdom

Although the recognition of a right to privacy in the United Kingdom is a fairly recent development, so far the provisions guaranteeing privacy rights have been construed positively to ensure protection. The recent adoption of privacy laws in United Kingdom's development of privacy rights illustrates the immediate revolutionary impact that legislation can have in correcting or improving the state of any laws. This is relevant in Nigeria where there are, at present, no laws regulating the protection of information processed in Internet cafes.

Regarding data, the United Kingdom Data Act, in accordance with the European Union Directive, sets out principles and contains several relevant features for any proposed data legislation in Nigeria, and in this case, for the protection of information processed in Internet cafes. There are however flaws in the supervision of the Act, which diminishes the protection available under it and underlines the importance of proper enforcement of any legislation.

10.1.2 United States of America

In the United States, there are established constitutional, tort law and other statutory privacy provisions, which have been successfully construed to provide privacy protection. However, many constitutional and tort law provisions guaranteeing the right to privacy have been construed narrowly by the courts resulting in the denial of protection in many cases. This highlights the essential role of the judiciary in the ultimate delivery of the benefits guaranteed under privacy protection provisions.

The main federal legislation regulating data protection in the United States is the Privacy Act,²⁰²⁶ whose operation is limited to the regulation of government activities and flawed in the failure to provide for proper regulatory and administrative measures to ensure its successful working. Similarly, the Freedom of Information Act,²⁰²⁷ which regulates the

²⁰²⁶ (1974) 5 U.S.C. Section 552a.

²⁰²⁷ (1966) 5 U.S.C. as amended.

collection, processing and disclosure of information by government and its agencies does not make provision for its effective administration to ensure compliance with these laws.

There are other federal and state laws which provide limited protection for (privacy and) data within the subject matter to which they relate. However, they are contained in different statutes, which are also periodically amended by different laws regulating information practices, rendering access to the law on data protection in the United States complicated.

It is clear from examination of the United States privacy and data laws that it is not sufficient to have provisions guaranteeing privacy and data protection in place. In order to provide any benefit, such provisions must be accessible, appropriately worded, constructively interpreted and applied by the courts and they must be efficiently administered.

To bring this home, any laws for the protection of privacy and data in Internet cafes in Nigeria must be accessible to the people, sufficiently detailed, they must contain provisions for its administration and will necessarily rely on the judiciary for positive and constructive application and for the development of its principles.

10.1.3 Germany

German law demonstrates the effectiveness of sound constitutional provisions and constructive judiciary interpretation in providing privacy protection. The essential role of the judiciary in legal development is also affirmed in the German Civil courts' construction of the Civil Code in privacy cases. German constitutional law privacy protection provides an ideal and constitutes a call for the provisions guaranteeing privacy in the Nigerian constitution to be better utilised.

The Nigerian constitutional provisions will be relevant both for general privacy protection and specifically for the protection of privacy and data in Internet cafes. The approach of the German courts to the interpretation of the available privacy provisions also should be viewed as a call for the Nigerian judiciary to be proactive and constructive in the interpretation and application of available privacy laws.

Germany's Data Protection Act contains detailed provisions for the protection of data and provisions regarding its administration. These data laws are consistent in terms of access, comprehensiveness, and supervision. The German Data Act also contains similar principles and features as the United Kingdom Act, which are vital for effective data protection and relevant in the protection of data in Internet cafes in Nigeria

10.1.4 South Africa

The protection of privacy in South Africa is largely hinged on the constitutional guarantee of privacy working with the Common Law. This has so far proved efficient,

applicable and developable to meet current privacy needs, and has been shown, will also cover Internet café privacy protection needs. The interaction and cooperation between the Constitution and Common Law for the protection of privacy provides an ideal example within a similar African context of the practicality and benefit of such a system.

Data protection is achieved in South Africa using the constitutional guarantee of privacy which also protects data where applicable and by means of various statutes, which are, mostly effective for their purpose. However, the need for a specific and detailed data Act recognising and incorporating international standards has been acknowledged in South Africa and is being addressed. In this regard, there is a proposed South African Data Protection Bill that incorporates data protection principles similar to those of the United Kingdom and the European Union that have been relied upon in this work as appropriate for Nigeria.

10.1.5 Nigeria

In Nigeria, neither the Constitutional nor the Common Law principles have been sufficiently developed to clearly define the ambit of the available privacy protection, either generally or with regard to Internet cafes. Data protection legislation is virtually non-existent and the available privacy/data law regulating Internet transactions is at present in draft form.

10.2 Overall Conclusion

On the basis of the preceding observations and conclusions, it is submitted that the development of the Nigerian constitutional provisions and the Common Law on privacy coupled with the enactment of a Nigerian Internet café privacy and data protection Act, integrating the principles in Chapter 9, will be of great benefit in the protection of information processed in Internet cafes.

With regard to privacy protection, the German, United States courts and the South African cases have demonstrated that constitutional provisions guaranteeing privacy provide a firm and stable foundation for the recognition of privacy rights. Furthermore, the courts in Germany and South Africa have shown that given suitably broad-based provisions, a wide variety of privacy invasion cases can be recognised, thus allowing the law to keep up with technological changes.

Since the Nigerian Constitution contains similar provisions to those in the German, United States and South African Constitutions, as well as the Human Rights Act, which have been shown to be considerably productive and competent for privacy protection, these should be developed and utilised. It may be safely presumed that a benevolent interpretation of these provisions will provide a common, solid, and reliable basis for the effectual protection of the right to privacy in general and the protection of information processed in Internet cafes in particular in Nigeria. The decisions of the United Kingdom,

United States, German and South African courts will also serve as valuable reference for the Nigerian courts.

As for data, given the absence of a data protection Act and the fact that the only available provisions on data protection in Internet cafes are contained in a draft law which has been shown to be essentially defective in vital areas, it has been established that there is a clear need for data protection laws and a law regulating the processing of information in Internet cafes. The common data protection principles previously identified embody the necessary features of a good data protection law and will provide a precedent in this regard.

The adoption of these principles in Nigeria will be beneficial in more than one way. Firstly, the new law will avoid the shortcomings identified in previously enacted laws, which the standards sought to amend. Secondly, if applied, the principles will not only enhance effective data protection in Nigeria, their adoption will also render Nigerian laws at par with other data laws that meet the international data protection standards. This will enhance the free flow of data for business and other relationships between Nigeria and such countries. Thus the broad base provided by the principles will serve as a guide in the drafting of a Nigerian data protection law and for the protection of privacy and data in Internet cafes in Nigeria.

As for the mode of supervision, a dual administrative system is suggested since this already operates in Nigeria and state supervisors may be able to better assess and deal

with affairs in their different states on the basis of knowledge of the different Internet café practices reflecting the stage of development in the states.

Although the practice in Internet cafes represents just an aspect of privacy and data protection, it is sufficiently significant and the possible damage from their invasion sufficiently grave to warrant attention. The protection of privacy and data are areas of the law that require definite, accessible, comprehensive, and enforceable legislative regulation, compatible with internationally recognised standards. It is submitted that for maximal effectiveness, the law regulating the practice in Internet cafes should also attain to the same standard. In this regard, it is affirmed that the implementation of the above propositions will produce up-to-standard privacy and data protection generally and with regard to information processed in Internet cafes in Nigeria.

APPENDIX

RESEARCH METHODOLOGY

1.1 Introduction

This work, “Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in Internet Cafes and Suggestions for Appropriate Legislation in Nigeria” entails an examination of South African and Nigerian and privacy and data laws in relation to the processing of information in Internet cafes. In this regard, examination of relevant Internet café practices in South Africa and Nigeria must be done.

Internet cafes are businesses that provide access to computers and a network that links computer networks all over the world by satellite and telephone, connecting users with service networks such as e-mail and World Wide Web. In addition to Internet access, computers in Internet cafes are also used for commercial typing and printing of documents such as Curriculum Vitae, students’ term papers, projects, theses, work applications among others.²⁰²⁸

²⁰²⁸ Cf above Para 1.4.

As mentioned above,²⁰²⁹ the processing of information in Internet cafes compounds the privacy risks inherent in Internet use, as common use of computers greatly increases intentional or accidental access to information processed by others. Furthermore, the mode of operation of Internet cafes allows Internet café staff ready access to information.²⁰³⁰ The aim of this aspect of the research is to establish the degree of usage of Internet cafes in South Africa and in Nigeria to gain knowledge of practices constituting threats to privacy in order to prescribe practical and relevant solutions for the privacy and data invasion problems identified.

Other issues to be determined are: the availability of Internet cafes for public use; the degree of usage of the Internet and e-mail facilities in Internet cafes; the awareness of users and Internet café owners, about the potential for invasion of privacy in the use of this technology in Internet cafes; and the degree of knowledge of Internet café users about available protection against invasions of privacy and data.

It is also intended to generally assess the degree of sensitivity of South African and Nigerian Internet café users to issues of privacy invasion. In this respect, questionnaires were designed and administered to Internet café users in South Africa and in Nigeria. Internet café owners, staff and users in South Africa and in Nigeria were also interviewed. In addition, university staff and students in both countries were interviewed. Below is an overview of the method by which the research was conducted.

²⁰²⁹ Para 1.4.

²⁰³⁰ Ibid.

1.2. Setting of the Study

In researching the topic, an empirical study was conducted in university towns in South Africa and in Nigeria on Internet and electronic mail use in both countries.

1.2.1 South Africa

In South Africa, the research was carried out in Pietermaritzburg, a town with a population of 9,426,018 in 2001.²⁰³¹ The choice of Pietermaritzburg, as research site was based on the fact that it is a University town, therefore offers a sizeable academic/elite population.

Another significant factor is that the research was conducted at a time of rapid growth in business and industries in Pietermaritzburg, notable among which was the opening of a shopping mall along a major highway in September 2004.

It was the researcher's thinking that the university and "business" population of Pietermaritzburg should offer a sizeable population of people that would need to establish or/and maintain family, businesses, academic and other relationships or transactions necessitating the use of the e-mail, and the Internet.

²⁰³¹ Wikipedia Contributors at http://schools-wikipedia.org/wp/s/South_Africa.htm. Accessed March 2008.

It was also the researcher's thinking that the relatively small size of the town would enhance the ability to be thorough in terms of covering the Internet cafes in the town. The Internet cafes used were selected according to availability at that time. In this regard, there was an Internet café situated close to the University of Kwazulu-Natal Pietermaritzburg, while many others were located in the city center.

1.2.2 Nigeria

In Nigeria, Ile-Ife, a University town in the South-West of Nigeria (Osun State), was the research site. Ile-Ife, like Pietermaritzburg, is a university town with established businesses and a population of 501,952 people in 2000.²⁰³² It therefore, like Pietermaritzburg, offered a manageable research population, and was an appropriate research site in terms of the population providing a combination of students, workers and business persons.

Lastly, having lived in Pietermaritzburg as well as in Ile-Ife, the researcher's previous knowledge of both towns considerably facilitated knowledge of, and transportation between, relevant locations for efficacious gathering of information for the research. This proved an additional benefit to choosing these sites.

1.3 Research Population

²⁰³² Wikipedia Contributors at <http://en.wikipedia.org/wiki/Ife>. Accessed March 2008.

The target population for this study was students of institutions of higher learning and workers, without any gender, age²⁰³³ or race specification. The rationale for focusing on this group of students, and young people is that, from the researcher's observation prior to conducting the study, a large percentage of Internet users in cyber-cafes are students and young people. This may be attributed to the need of students to source information in their search for better education, or the need for jobs (within the country and abroad), the need to maintain family and other relationships, and the need for entertainment such as computer or Internet games, among other reasons. These groups of people are also often away from family and have the need to keep in touch.

1.4 Data Collection

Data collection, which was qualitative rather than quantitative, entailed formulating and collating questions for questionnaires and interviews. 100 questionnaires were distributed in each country in the expectation that at least 40 would be validly filled, returned and be usable. The questionnaires were distributed to users of e-mail and other Internet facilities in Internet cafes. Questionnaires were also left on the reception counters to be picked up by customers in some Internet cafes where this was allowed. These were to be filled by those customers who came in the researcher's absence.

²⁰³³ Although age was not relevant for the purpose of this research and as such was not factored into the questionnaire, most people in this category are younger than 50 years old.

The data collection process involved the researcher being present at designated Internet cafés between 9am and 6pm three days a week, during which time interviews were conducted and questionnaires administered to users as well as owners of the Internet cafes. Five Internet cafes were visited in South Africa and five in Nigeria. With the permission of the owner, the researcher sat at Internet cafes waiting for prospective Internet users.

When they arrived, customers were given a few minutes to settle at the computer after which the researcher walked up to each participant, briefly explained the project and in most cases, customers agreed to fill the questionnaires. In some cases, they preferred to have the questions asked and their answers written down by the researcher. Interviews were also administered to Internet café owners and in some cases, their managers. In addition, general observations²⁰³⁴ relevant to the study were made and notes taken while sitting in the Internet cafes.

Further to this, a brief survey was conducted to assess the degree of reliance of university lecturers on Internet cafes. In this regard, lecturers in the department of Medicine and the faculty of Law were chosen. It was the researcher's reasoning that her previous acquaintance with some of the staff in both departments in South Africa as well as in Nigeria would facilitate straightforward access to the lecturers for interview purposes. This proved rewarding and the interviews were conducted without any problems.

²⁰³⁴ Such as the lay-out of the Internet cafes, procedure for customer access to the facilities, proximity of other customers to the computers being used and factors that might have a bearing on privacy.

University students were also interviewed to assess their degree of reliance on Internet café services. As there were no restrictions in terms of age, gender, or any factor other than being a university student, this was done by random sampling. The researcher stood outside the university library between 12noon and 2pm for 2 days, interviewing students.

1.5 Research Instrument

The questionnaires²⁰³⁵ and the interviews²⁰³⁶ were the instruments used in carrying out the quantitative research. The interview format was developed in a way that allowed the interviewee to respond to the question explicitly and without bias. Both the questionnaires and the Internet café interviews addressed the same issues, with the main difference being that the interview questions were framed from the perspective of the Internet café owner/ manager, (data controller).

In addition, the participant could expand on any given point, check with the researcher about the specific purport of any question and receive immediate feedback as to whether the question had been interpreted correctly. On the other hand, with the questionnaires, where the participants did not ask any questions, the researcher had no opportunity to checkout with them to clarify any uncertainties.

²⁰³⁵ Cf Annexure A.

²⁰³⁶ Annexures B and C. Some of the Internet café customers chose to be interviewed instead of filling out the questionnaire by themselves. In such cases, the questions in Annexure A were administered orally and answers recorded by the researcher.

The Internet café interviews took a face-to-face format and questions were direct, and worded so that they could be easily understood. There were 10 prepared questions. In the interviews, respondents were asked questions and their responses were recorded on tape to be processed for data analysis. The interview questions were encoded unambiguously and they were arranged to facilitate logical and smooth progression of the interview. The same straightforward, logical and sequential format of questions was adopted for the questionnaire.

The questionnaire consisted of 11 questions. Some of the questions supplied options or categories from which answers could be chosen. These provided participants with ready-made responses and facilitated grouping and coding in analyzing the data. Some other questions were open-ended to allow the respondents to express themselves in their own words. There were also follow-up questions designed to check out the participants' understanding of particular questions and confirm data consistency. In all cases, the anonymity and protection of their privacy was guaranteed to the participants.

The questions asked in the survey and random sampling were brief, few and to the point. There were six prepared questions in total and each interview lasted an average of 9 minutes.

1.6 Data Analysis and Findings

The researcher's aim was to be able to analyse 100 questionnaires (50 questionnaires per research site but in any case, no less than 40 per site). Out of the 200 questionnaires given out, a total of 129, (61 in South Africa and 68 in Nigeria) were returned properly filled and usable. The data derived from the questionnaire was analysed by searching for patterns among the data generated. The following are some of the findings from the data analysed.

1.6.1 The Questionnaires

1.6.1a South Africa

In South Africa, these findings²⁰³⁷ were derived from analysis of the questionnaire:

- (1) 81% of the Internet café users were students, 15% were workers, and job seekers made up the last 4% of Internet café users.
- (2) 9% of the Internet café users interviewed used Internet cafes daily, 48% weekly, and 43% monthly.
- (3) 53% of the research population made use of more than one Internet café in a two-month period.
- (4) 22% of Internet café users thought that the use of Internet cafes posed any threat to their privacy.

²⁰³⁷ These findings have been applied in the body of the thesis. See Para 1.4.

(5) 17% of such Internet café users mentioned the possibility of invasion of their privacy in Internet cafes by peeping toms.²⁰³⁸

1.6.1b Nigeria

In Nigeria,

- (1) 66% of the Internet café users in Nigeria were students, 22% were workers and 12% were graduates seeking jobs
- (2) 13% of the Internet café users in Nigeria made use of Internet cafes daily, while 54% used them weekly and another 33% monthly
- (3) 96% of the Internet café users in Nigeria made use of more than one Internet café within a two- month period.
- (4) 46% of the Internet café users interviewed were aware of the potential for invasions of their privacy in Internet cafes.
- (5) 90% of the Internet café users who thought the use of Internet cafes posed a threat to privacy gave the example of peeping passers-by as a way in which privacy could be invaded.

The analysed data has been placed into categories and discussed around relevant themes in the thesis.²⁰³⁹

²⁰³⁸ Cf below Para 1.4.

²⁰³⁹ See for example Chapter 1 Para 1.4. The findings are mostly relevant in the laying of the foundation of this work thus references to the research findings are more copious in the early chapters of this work.

1.6.2 The Internet Café Interviews

The data derived in response to the interviews questions was analysed by transcribing the information that was recorded in the interview process. The transcripts were then analysed by searching for patterns among the data.

1.6.2a South Africa

In South Africa,

- (1) 90% of the Internet café owners interviewed were of the opinion that the use of Internet cafes held a risk of invasion of privacy
- (2) 100% of the Internet café owners identified “incorrect logouts” by the clients as the main factor responsible for/ enhancing invasion of privacy.
- (3) 20% of the owners thought that technical measures could be taken by Internet café owners to prevent invasions of customers’ privacy

1.6.2b Nigeria

In Nigeria, the results of the Internet café interviews showed that:

- (1) All the Internet café owners were aware of threats to privacy

- (2) All of them identified incorrect logout by clients, and third- party hacking as the main threats to privacy
- (3) 20% of the owners mentioned the option of Internet café owners taking technical measures to ensure the protection of customers' privacy.

1.6.3 The Survey

1.6.3a South Africa

The research produced the following results in South Africa:

- (1) All the doctors in the department of Surgery, Greys Hospital, Pietermaritzburg used e-mail and Internet facilities at least 4 times a week and
- (2) All of them had ready access to the Internet at work or, and at home therefore none of them relied on Internet cafes for Internet access or e-mail.

Similarly all the lecturers in the School of Law, Pietermaritzburg used the Internet and e-mail facilities at least 4 times a week and they all had ready Internet access at work or, and home, therefore none relied on Internet cafes for Internet access.

In South Africa, the results derived from analysis of the student sample indicated that:

(1) 86% of students who sent and received mail and surfed the Internet did so at least 10 times a week. (Some checked their e-mails about 3 times a day).

(2) All the students had access to the Internet and e-mail facilities on the university computers at the student LANs. However, 27% of these students used Internet cafes occasionally (no more than twice a month).

1.6.3b Nigeria

The survey conducted in the department of Medicine of the Obafemi Awolowo University in Nigeria to determine the degree of reliance on Internet cafes among the lecturers revealed that:

(1) All the doctors used e-mail facilities at least twice a week

(2) 92% of the doctors relied on Internet cafes (including the university LAN)²⁰⁴⁰ for Internet access and to send and receive Internet mail.

Similarly, in the Faculty of Law of the Obafemi Awolowo University, the survey revealed that:

(1) All the lecturers used e-mail facilities at least twice a week

²⁰⁴⁰ The researcher observed that the university LAN was set up like an Internet cafe in the sense that it offered a total of about 15 computers with no significant physical structures to prevent others from seeing or reading information being processed on the computers. In addition, like other Internet cafes, students and staff paid for services at the time of use and technical support was provided by staff within the premises.

(2) 91% of the lecturers depended on Internet cafes and the university LAN for their Internet access needs.

As for the student sample, the findings were that:

(1) 73% of the students in the Obafemi Awolowo University who sent and received mail and surfed the Internet did so at least once and no more than 3 times a week.

97% of these relied on Internet cafes including the university LAN for their Internet access needs.

The above findings establish significant use of the facility in South Africa and an even greater degree of reliance on Internet cafes in Nigeria than in South Africa. These results are sufficient to validate our focus on Internet café privacy in both countries and also useful for comparison as well as contrast purposes in the work. All the data analysed was coded and placed under descriptive categories and issues raised have been discussed around the themes and sub-topics under which they fall in this work.²⁰⁴¹ As this was a qualitative research, there was no need for the use of a statistical package to analyse the data.

1.7 Validity and Reliability

The researcher ensured the validity of the research by employing qualitative research methods to collect the required data, using structured open questions, as well as closed questions where appropriate. The questions asked were straightforward and

unambiguous, such that they could be easily interpreted. These questions were administered in form of questionnaires and interviews.

The questionnaire and Internet café interview drafts were checked by the research supervisor, Prof David McQuoid-Mason of the department of Clinical and Procedural Law, Howard College School of Law, University of Kwazulu-Natal, Durban. In addition, 10 first year BA English students in the University of Kwazulu-Natal, Pietermaritzburg completed the questionnaires as a pilot to assess the comprehensibility of the questions and validity of information received. Information gained from the pilot test was all consistent and relevant. The feedback received from the interviews conducted also affirmed that the questions were understood and interpreted accurately, and, as intended.

The nature of the research, and the questions asked did not require the giving of intimate or personal information. As such, the questions asked in the questionnaire and the interviews were generally, not perceived as offensive or intrusive into personal space. It is thus believed that the questions were answered accurately, honestly and in sufficient detail. From the above, it may safely be asserted that if the research were repeated under similar circumstances, the results derived would be consistent and the researcher would draw the same conclusions. It is thus affirmed that the data collected and presented is reliable and the research can be taken to be credible.

1.8 Ethical Issues

²⁰⁴¹ Cf above Para 1.4 at pp 21ff

Before commencing the data collection process, the researcher sought and obtained the permission of each Internet-café owner as well as the individual users to be interviewed. The Internet-café owners and users were given clear explanations as to the nature and purpose of the research and were informed that participation was voluntary. Thus, should any respondent feel uncomfortable or be unwilling he or she could refuse to participate in the research process or withdraw at any time after agreeing to participate. In addition, prospective participants were assured of confidentiality and anonymity.

The questionnaire also contained a written explanation guaranteeing confidentiality and anonymity. To give effect to this, the questions asked in the questionnaire and the interviews did not require the giving of personal demographic information such as name, date of birth, address, gender, race or any other identifying personal information relating to participants.

1.9 Difficulties and Observations

Although there were no incidences of unwillingness to respond arising from the nature of the research and the questions asked, other problems and setbacks were encountered. There were cases where customers declined participation because, according to them, they were in a hurry.

Also, both in South Africa and Nigeria, some Internet café owners did not spend much time in their Internet shops. They employed shop managers who managed and worked

with the technology. In many such cases, the owners were unavailable, and when available, they were reluctant to fill the questionnaires or do the interviews, as they felt inadequate in terms of actual working experience in the Internet café to answer the questions. In some cases, the shop managers and the owners each filled the questionnaires and did the interview.

In addition, in South Africa, one Internet café owner displayed a reluctance to answer any questions or allow the researcher to administer questionnaires to customers in her Internet café. She suggested instead that the researcher stay in the corridor of the mall in which the Internet café was situated and accost potential clients because, according to her, “people do not pay to come and get harassed in here.” It was not a viable option to accost potential clients in the corridor, as it was difficult to tell who among those walking along the corridor was going into the Internet café or any of the other shops around, and it would constitute a physical obstruction to stand in front of the door, amongst several other problems attending that suggestion.

This constituted a slight set back as this Internet café was the closest to the university that the researcher had identified and relied on to get a considerable population of university student participants. In the final analysis however, the results were in no major way affected. The researcher found another Internet café in town to conduct the research in, and overall, university students emerged as the highest population of users in all the cafes visited.

Another setback encountered was the inconsistent rate at which customers came into the Internet cafes. Sometimes, there were no customers to check e-mail or use the Internet in an Internet café between 8am and 2pm in a day. (Some of the other facilities such as typing, photocopying, printing, public telephone services and the purchase of stationary were more often utilised by customers than Internet services). It was discovered that more customers used e-mail and Internet facilities after school or work hours, specifically between 4pm and 6pm. However, there was no guarantee of getting any Internet users at any specific time on any day and daily waiting for prospective Internet users made the research process slow and tedious.

On certain days when the researcher could not be at certain Internet- cafes between 4pm and 6pm, she left some of the questionnaires in the café to be filled by customers. Some of the questionnaires left at the cafes were returned incompletely filled. The researcher then had to disregard the incomplete questionnaires where key questions were left unanswered. However, some of these problems such as the irregular and unpredictable timing of customers at the cafes and incompletely filled questionnaires had been anticipated.

1.10 Conclusion

The following emerges in conclusion. The number of questionnaires well completed and returned exceeded the projected amount, giving an excellent overall return on the questionnaires. As for the Internet café interviews, 90% of the owners/managers of the

Internet cafés visited were interviewed, yielding relevant data. The lecturer and student interviews conducted also yielded satisfactory feedback in terms of meeting their objective for being carried out; the needed information was obtained. The setbacks mentioned in Paragraph 1.9 above were only temporary and did not affect overall data collection. Furthermore, after analysis, the data received from the questionnaires appeared consistent. It may thus be concluded that the research was conducted successfully.

ANNEXURE A**COPY OF QUESTIONNAIRE ADMINISTERED TO INTERNET CAFÉ
CUSTOMERS**

This questionnaire is prepared strictly for academic purposes. No information from which the participant may be identified is required in the questionnaire. While there is no obligation to complete this questionnaire, your cooperation in carefully completing it will be highly appreciated. Thank You.

(1) What is your present occupation? (Circle the applicable category/ies)

(a) Student (b) Worker (c) Unemployed (d) Other (Specify).

(2) How often do you use Internet cafes? (Circle the most appropriate)

(a) Daily (b) Weekly (c) Monthly (d) Occasionally (Please specify)

(3) How many different Internet cafes have you ever used?

(a) 1 (b) 2 (c) 3 (d) 4 or more

(4) How many Internet cafes do you frequently use?

(5) "Frequent use" of Internet cafes, for me, means (Circle the most appropriate)

(a) Daily (b) Weekly (c) Monthly (d) Other (Please specify)

(6) What facilities do you frequently use in an Internet cafe?

(7) Do you think the use of Internet cafes creates a risk or threat to personal privacy?

(8) If yes, in what way does the use of Internet cafes create risks to personal privacy?

(Please explain/give examples)

(9) What are the risks to privacy caused by the use of Internet cafes?

(10) Do you think anything can be done to minimise these risks?

(11) If yes, what can be done to minimise the risks to personal privacy caused by the use of Internet cafes? (Please explain/ give examples)

ANNEXURE B

INTERVIEW QUESTIONS ADMINISTERED TO INTERNET CAFÉ OWNERS

- (1) How long have you owned this business?
- (2) Is the Internet café the only service you offer within these premises?
- (3) If no, what other services do you offer in this shop?
- (4) What type of services do customers require or use on the computers?
- (5) Who is your largest category of customers? students, workers, retired, others?
- (6) Do customers need help to use the computers?
- (7) How often do customers need help to use the computers? -usually, often or seldom
(explain/expand)
- (8) Do you think there are any threats or risks to customers' privacy in the use of these Internet cafe computers?
- (9) Give examples
- (10) What can be done to prevent improper access to customers' information or invasions of privacy?

ANNEXURE C

QUESTIONS ASKED IN THE LECTURER /STUDENT SURVEY

- (1) Do you have a personal computer in your office?
- (2) Do you have access to a personal computer at home?
- (3) Generally, what facilities do you use on the computer? E.g e-mail, projects, papers,
Internet browsing
- (4) Do you use Internet cafes?
- (5) How regularly?
- (6) What facilities do you generally use in Internet cafes?

BIBLIOGRAPHY

BOOKS AND ENCYCLOPAEDIA

- Aguda: *The Law of Evidence* (1989) 3rd ed. Spectrum Law Publishing Ibadan.
- Amerasinghe C. F. *Aspects of the Actio Injuriarum in Roman-Dutch Law* (1966) Lake House Investments Ltd Colombo.
- American Jurisprudence 2d Constitutional Law (1979).
- American Law Institute *Restatement (First) of the Law* (1995) American Law Institute Publishers Philadelphia.
- American Law Institute *Restatement (Second) of Torts* (1977) American Law Institute Publishers Philadelphia.
- American Law Institute *Restatement of Torts* (1939) American Law Institute Publishers Philadelphia.
- Asein J.O. *Introduction to Nigerian Legal System* (1998) Sam Bookman Publishers Ibadan.
- Baer R. M. *The Digital Villain* (1972) Addison-Wesley Publishing Co London.
- Birkinshaw Patrick *Freedom of Information: The Law, the Practice and the Ideal* (2001) Butterworths London.
- Birkinshaw Patrick *Government & Information: The Law Relating to Access, Disclosure & Regulation* (1990) Butterworths Edinburgh.

- Birks P. (ed) *Privacy and Loyalty* (1997) Clarendon Press Oxford.
- Brazier M.R., Alexander D., Buckley R.A., Burrows A.S., Carty H.F., Dugdale A.M., Mulholland M., Tettenborn A, Lord Wedderburn of Charlton (eds) *Clerk & Lindsell on Torts* (1995) 17th ed Sweet & Maxwell London.
- Bulos M. & Sarno C. *Codes of Practice and Public Closed Circuit Television Systems* (1996) Local Government Information Unit London.
- Burchell Jonathan *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum* (1998) Juta & Co Ltd Kenwyn.
- Buys Reinhardt (ed) *Cyberlaw@ SA II: The Law of the Internet in South Africa* (2004) 2nd ed Van Schaik Pretoria.
- Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D, Woolman S *Constitutional Law of South Africa* (2004) Juta & Co Ltd Cape Town.
- Cohn E. J. *Manual of German Law 1968* 2nd ed Vol 1 (1990) British Institute of International and Comparative Law London.
- Currie David P. *The Constitution of the Federal Republic of Germany* (1994) The University of Chicago Press London.
- De Waal Johan, Currie Iain, Erasmus Gerhard *The Bill of Rights Handbook* (2000) 3rd ed Juta & Co Ltd Kenwyn.
- Dugdale A.M. *Clerk & Lindsell on Torts* (2000) (General ed) Sweet & Maxwell London.

- Edelstein Ludwig *The Hippocratic Oath: Text, Translation, and Interpretation* (1943) Johns Hopkins Press Baltimore.
- Garfinkel Simon *Database Nation: The Death of Privacy in the 21st Century* (2000) O'Reilly and Associates Sebastopol Beijing.
- Grosz Stephen, Beatson Jack, Duffy Peter *Human Rights The 1998 Act and the European Convention* (2000) Sweet & Maxwell London.
- Gurry Francis *Breach of Confidence* (1984) Clarendon Press Oxford.
- Henderson Harry *Privacy in the Information Age* (1999) Facts on File Inc New York.
- Heuston R.F.V. and Buckley R.A. *Salmond and Heuston on the Law of Torts* (1992) 20th ed Sweet and Maxwell London.
- Hoffmann L.H. & Zeffert D.T. *The South African Law of Evidence* (1998) 4th ed Butterworths Cape Town
- Holbrook James *Ten Years Among the Mail Bags* (1855) Philadelphia Press Philadelphia.
- Holland T.E. *Jurisprudence* (1895) 8th ed Clarendon Press Oxford.
- Hornby A.S. *Oxford Advanced Learner's Dictionary* (2001) 6th ed Oxford University Press Oxford.
- Justice Report *Privacy and the Law* (1970)
- Keeton P. & Keeton R.E. *Cases and Materials on the Law of Torts* (1977) 2nd ed West Publishing Co St Paul Minnesota.
- Keeton W.P., Dobbs D.B., Keeton R.E. & Owen D.G. *Prosser and Keeton on the Law of Torts* (1984) 5th ed West Publishing Co St Paul Minnesota.

- Kindersley Dorling *Illustrated Oxford Dictionary* (2003) edn Oxford University Press Oxford.
- Kodilinye G. S. *Kodilinye: The Nigerian Law of Torts* (1982) Sweet and Maxwell London.
- Kodilinye G. & Aluko O. *Kodilinye: The Nigerian Law of Torts* (1999) 2nd ed Spectrum Books Ltd Ibadan.
- Kohler J. *Personlichkeitsrecht* v 1.
- Kommers Donald P. *The Constitutional Jurisprudence of the Federal Republic of Germany* (1997) 2nd ed Duke University Press London.
- Lipschultz J.H. *Free Expression in the Age of the Internet; Social and Legal Boundaries* (2000) Westview Press Boulder.
- Locke John *An Essay Concerning Human Understanding* (1995) Prometheus Books New York.
- Locke John *The Second Treatise of Civil Government* (1986) Prometheus Books New York.
- Lunney Mark and Oliphant Ken *Tort Law (Text and Materials)* (2003) 2nd ed Oxford University Press Oxford.
- Marett Paul *Intellectual Property Law* (1996) Sweet & Maxwell London.
- Markesinis B.S. (ed) *Protecting Privacy* (1999) Oxford University Press New York.
- Markesinis B.S. *The German Law of Torts* (1990) 2nd ed Clarendon Press Oxford.

- Marsh Norman (ed) *Public access to Government-Held Information* (1987) Stevens & Sons Ltd London.
- McClellan S. Grant *The Right to Privacy* (1976) The Reference Shelf Volume 48 Number 1 New York.
- McKerron R.G. *The Law of Delict* (1971) 7th ed Juta & Co Ltd Cape Town.
- McQuoid-Mason D.J. *The Law of Privacy in South Africa* (1978) Juta & Company Ltd Johannesburg.
- Mill John Stuart *Utilitarianism Liberty Representative Government* (1962) Everyman's Library J.M. Dent & Sons London.
- Neethling J. *Neethling's Law of Personality* (2005) 2nd ed Butterworths Durban.
- Neethling J. *Persoonlikheidsreg* (1985) Butterworth Durban.
- Neethling J., Potgieter J.M., & Visser P.J. *Law of Delict* (2006) 5th ed Butterworths Durban.
- Newman E. & McQuoid-Mason D.J. *Lee and Honore The South African Law of Obligations* (1978) 2nd ed Butterworths Durban.
- Nicol A., Millar G., Sharland A. *Media Law and Human Rights* (2001) Blackstone Press Ltd London.
- Nora S. & Minc S. *The Computerization of Society* (1981) MIT Press England.
- Norris C. & Armstrong G. *The Maximum Surveillance Society; The Rise of CCTV* (1999) Berg Oxford.

- O' Higgins P. *Cases and Materials on Civil Liberties* (1980) Sweet & Maxwell London.
- Owen R. *Essential Tort Law* (2000) 3rd ed. Cavendish Publishing Ltd Sydney.
- Palmer Norman *Confidentiality and the Law* (1990) Lloyd's of London Press Ltd.
- Pearson H. & Miller C. *Commercial Exploitation of Intellectual Property* (1990) Blackstone Press Ltd London.
- Phillips J. & Firth A. *Introduction to Intellectual Property Law* (1995) 2nd ed Butterworths London.
- Reed Christopher *Internet Law: Text and Materials* (2004) 2nd ed Cambridge University Press Cambridge.
- Richardson S. S. *Notes on the Penal Code Law (Cap 89 Laws of Northern Nigeria, 1963)* (1987) 4th ed Oxford University Press Oxford.
- Robertson Mike (ed) *Human Rights for South Africans* (1991) Oxford University Press Cape Town.
- Rogers W.V.H. (ed) *Winfield and Jolowicz on Tort* (1994) 14th ed Sweet & Maxwell London.
- Roos Anneliese *The Law of Privacy (Data) Protection: A Comparative and Theoretical Study* (2003) University of South Africa.
- Samovar L.A. & Porter R.E. *Intercultural Communications: A Reader* (1994) International Thompson Publishing Belmont CA.

- Sanni A.O. (ed) *Introduction to Nigerian Legal Method* (2006) Obafemi Awolowo University Press Ltd Ile-Ife.
- Sloan I. J. *Law of Privacy Rights in a Technological Society* (1986) Oceana Publications Inc. New York.
- Torpey John *The Invention of the Passport: Surveillance, Citizenship and the State* (2000) Cambridge University Press Cambridge.
- Van der Walt J.C. *Delict: Principles and Cases* (1979) Butterworths Durban.
- Van Wyk D, Dugard J, De Villiers B, Davis D *Rights and Constitutionalism: The New South African Legal Order* (1994) Juta & Co Kenwyn Cape Town.
- Von Bar Christian *The Common European Law of Torts* Volume 1 (1998) Oxford University Press New York.
- Wacks Raymond *Privacy and Press Freedom* (1995) Blackstone Press Ltd London.
- Wacks Raymond *The Protection of Privacy* (1980) Sweet & Maxwell London.
- Wadham J & Mountfield H *Blackstone's Guide to the Human Rights Act 1998* (1999) Blackstone Press Ltd Oxford.
- Walker D M *The Law of Delict in Scotland* (1966) V II.W Green & Son Edinburgh.
- Weir Tony *A Casebook on Tort* (1992) 8th ed Thomson Professional Publishing Canada.

- Westin A F *Privacy and Freedom* (1967) Lowe and Brydone Ltd London.
- Wright C *Cases on the Law of Torts* (1967) 4th ed Butterworths.

ARTICLES, JOURNALS AND PERIODICALS

- Anderson C. et al “Leading Cases” (2001) 115 *Havard Law Review* (No 1) 306.
- Bricout R.G. “The Preservation of Secrecy Provisions: Still Worth It?” (2002) *Acta Juridica* 247.
- Bloustein E.J. ‘Privacy as An Aspect of Human Dignity: An Answer to Dean Prosser’ (1964) 39 *New York University Law Review* 962.
- Byers S. The Internet: Privacy Lost, Identities Stolen (2001-02) 40 *Brandeis Law Journal* 141.
- Craig P. “The Courts, the Human Rights Act and Judicial Review” (2001) 117 *Law Quarterly Review* 589.
- D.A. Ijalaye “The Sociological School of Jurisprudence and the Nigerian Legal Order” (1992) *Nigeria and the Challenge of Knowledge* (Essays in Honour of Jonathan Olusesan Dipeolu) 33.
- Feldman D. “The Developing Scope of Article 8 of the European Convention on Human Rights (1997) *EHRLR* 266, 272.
- Forst Rainer “How not to Speak About Identity: The Concept of the Person in a Theory of Justice” *Philosophy and Social Criticism* (1992) Vol. 8 No 1.

- Foster S. “The Right to Private Sexual Life under Article 8 of the European Convention on Human Rights: *ADT v U.K.*” (2001) 35 *Law Teacher* (No 1) 76.
- Fried C. “Privacy” (1968) 77 *Yale Law Journal* 475.
- Joubert W. A. “Die Persoonlikheidsreg: ‘n Belangwekkende Ontwikkeling in die Jongste Regspraak in Duitsland” (1960) *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 23.
- Krause H. D. “The Right to Privacy in Germany- Pointers for American Legislation?” (1965) *Duke Law Journal* 481.
- McQuoid-Mason D.J. “Invasion of Privacy: Common Law v Constitutional Delict- Does It Make a Difference?” (2000) *Acta Juridica* 253.
- Neill B. “The Protection of Privacy” (1962) 25 *Modern Law Review* 393.
- Phillipson G. & Fenwick H. “Breach of Confidence as a Privacy Remedy in the Human Rights Act Era” (2000) 63 *Modern Law Review* 660.
- Oyedeji Foluke O. “The Influence of Natural Law on the Nigerian Legal System” (1998) (unpublished LL.M thesis)
- Prosser W. L. “Privacy” (1960) 48 *California Law Review* 383.
- Ruebhausen O. M. and Brim O. G. “Privacy and Behavioural Research” (1965) 65 *Columbia Law Review* 1184.
- Schwartz Paul M. “German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance” (2003) 54 *Hastings Law Journal* 751.

- Stuckey “The Equitable Action for Breach of Confidence: Is Information Ever Property?” (1981) 9 *Sydney Law Review* 402.
- Warren S. D. and Brandeis L. D. “The Right to Privacy” (1890) 4 *Harvard Law Review* 194.
- Wilkinson T. “Is Anyone Listening to Me?: *Bartnicki v Vopper*” (2003) 63 *Louisiana Law Review* (No 2) 589.
- Winfield P.H. “Privacy” (1931) 47 *Law Quarterly Report* 23.

INTERNET SOURCES

- American Civil Liberties Union “National ID Cards: 5 Reasons Why They Should be Rejected” (2002)
http://archive.aclu.org/issues/privacy/national_ID_Feature.html
- American Civil Liberties Union “National Identification Cards: Why Does ACLU Oppose a National ID Card System?” (1996)
<http://www.aclu.org/library/aaidcard.html>
- Banisar D. and Davies S. “Privacy and Human Rights: ‘An International Survey of Privacy Laws and Practice’ (1999)
<http://www.gilc.org/privacy/intro.html>
- Banisar D. ‘Privacy and Human Rights 2001’ (2001) <http://www.privacy.org/pi/summary/phr2000/threats.html#heading2>.

- Currie Iain “The NCA and the Proposed Protection of Personal Information Act” The Mandela Institute (2006)
<http://wwwserver.law.wits.ac.za/mi/privacy/nationalcreditact.htm>
- Electronic Privacy Information Centre “National Identification Cards” (2002) *http://www.epic.org/privacy/id_cards/default.html*
- Erickson W, Lloyd-Jones T, Theis M, Greatbatch I, Mulyawan B, Yunusa M.B, Adenekan S, Hasan A, Monteiro C, Dantas N, Sobriera F, Batty M “Mapping Urbanization for Urban and Regional Governance” Final Report DFID Research R8130 Research R8130, Max Lock Centre, University of Westminster(2003)
http://www.wmin.ac.uk/builtenv/maxlock/mapping/Report_for_Web/Word_final/1_Summary_MU.doc
- [Germany]: The (German) Federal Data Protection Act (1990)
http://www.bfd.de/information/engl_corner.html.
- [Germany]: Website of the Federal Data Protection Commissioner
<http://www.bfd.bund.de/>

- Green Paper on Electronic Commerce for South Africa Theme 2- “Building Trust in the Electronic Economy” Chapter 7 (2000)
http://www.polity.org.za/html/govdocs/green_papers/greenpaper/theme2.html#7
- Michalson’s Guide to Data Privacy Law in SA *<http://www.michalson.com/docs>* (2006)
- [Nigeria]: Research and Markets Mobile Africa (Market research report) (2006) *<http://www.mobileafrica.net/a70.htm>*
- Ohigheoga Eijeagbon “Nigeria: New Wire Tapping, Cyber Crimes Bill in Nigeria” (2006) *<http://lists.jammed.com/ISN/2006/10/0090.htm>*
- Oserogho E.O. “New Wire Tapping, Cyber Crimes & Anti-Terrorism Bill In Nigeria” (2006)
<http://www.legalbrief.co.za/article.php?story=20061013091452442>
- Privacy International “National ID Cards” (2002)
<http://www.privacyinternational.org/issues/idcard/>
- Otitie O. “Nigeria’s Identifiable Ethnic Groups” (1998)
<http://www.onlinenigeria.com/tribes/>
- Regulation of Interception of Communications and Provisions of Communication Related Information Act, 70 of 2002
- *<http://www.info.gov.za/gazette/acts/2002/a70-02/a70-02a.pdf>*.

- South African Government Information “Media Statement by the South African Law Commission Concerning Its Investigation into Privacy and Data Protection” (2002) <http://www.info.gov.za/speeches/2002>
- “South Africa Urged to take the Lead in Updating Privacy Laws for Internet” (1999) <http://www.itweb.co.za/sections/techforum/1999/991106810115.asp>
- The South African Law Reform Commission Discussion Papers (2005) <http://www.doj.gov.za/salrc/dpapers.htm>
- The South African Law Reform Commission Issue papers “Summary of Proposals and Questionnaire Issue Paper 24”(2003) http://www.doj.gov.za/salrc/ipapers/ip24_prj124/ip24_prj124_2003_sum_questions.pdf.

- Travis A “ID Cards: Un-British or Vital? The ID Debate” *The Guardian* 25 September 2001 at <http://politics.guardian.co.uk> .
- Wikipedia contributors: “Directive 95/46/EC on the protection of personal data” Wikipedia, The Free Encyclopaedia at http://en.wikipedia.org/wiki/directive_95/46/EC_on_the_protection_of_personal_data
- Williams B “Rulers Discuss Issuing National ID Cards” *The Militant* (2001) Vol 65 No35 <http://www.themilitant.com>
- Zamfara State of Nigeria Sharia Penal Code Law <http://www.zamfaraonline.com/sharia/chapter08.html>

MAGAZINES AND NEWS ARTICLES

- Aregbeyen Segun “Nigeria Lacks Legal Protection Against Piracy on the Internet” *The Comet* 25 October 2000
- (Case of) “*Gloria Mowarin v A.G. of the Federation*” *The Guardian* 20 Feb 1991
- (Case of) “*Sheen v Clegg*” *Daily Telegraph* 22 June 1961
- Cohen A. “Spies Among Us” *Time* 31 July 2000
- Farham A. “How Safe Are Your Secrets?” *Fortune* 8 September 1997
- Quittner J “Invasion of Privacy” *Time* 25 August 1997
- Shapshak David *Mail and Guardian* 24 April 1998

OTHER DOCUMENTS

- African [Banjul] Charter on Human and People's Rights, adopted June 27, 1981, O.A.U. Doc. CAB/LEG/67/3 rev.5,21 I.L.M. 58 (1982)
- The South African Law Reform Commission Discussion Papers: Discussion Paper 109 Project 124
- Green Paper on Electronic Commerce (South African Government Department of Communications)
- House of Lords Debates (1961) Vol. 229 Col 638
- International Commission of Jurists Conclusions of the Nordic Conference on the Right to Privacy (1967)
- The Online Thesaurus (Microsoft Office Word 2003 program)

TABLE OF STATUTES**CONSTITUTIONS****Algeria**

- Constitution of the People's Democratic Republic of Algeria (1989) as amended by the constitutional revision of 1996

Angola

- Constitutional Law of the Republic of Angola (1992)

Burundi

- La Constitution de la Republique du Burundi Promulgue le 13 mars 1992 ainsi que Decret- loi no 1/001/96 du Septembre 1996

Cameroun

- La Constitution du Cameroun Loi no 96-06 du 18 Janvier 1996

Ethiopia

- Constitution of the Federal Republic of Ethiopia (1994)

Germany

- *Grundgesetz fur die Bundesrepublik Deutschland* Vom 23 Mai 1949
(Basic Law for the Federal Republic of Germany 1949)

Mozambique

- Constitution of Mozambique 1990 as amended through 2004

Namibia

- Namibia Constitution adopted on February 1990

Niger

- Constitution du 18 Juillet 1999 Promulguée par décret du 09 Août 1999, du United Nations

Nigeria

- The 1979 Constitution of the Federal Republic of Nigeria
- The Constitution of the Federal Republic of Nigeria (Promulgation) Decree No 12, 1989
- The Constitution of the Federal Republic of Nigeria 1999

Rwanda

- Constitution of Rwanda 1991 adopted 1995

South Africa

- Constitution Act 108 of 1996
- Interim Constitution Act 200 of 1993

Uganda

- Constitution of the Republic of Uganda 1995 as amended by the Constitutional Amendment Act No 2 of 2005

United States of America

- Federal Constitution (Bill of Rights 1749):
 - First Amendment
 - Third Amendment
 - Fourth Amendment
 - Fifth Amendment
 - Ninth Amendment
 - Fourteenth Amendment

United States of America State Constitutions

Alaska

- The Constitution of the State of Alaska 1972 adopted Feb 5, 1956, Operative January 3, 1959, amended 1972

Arizona

- Constitution of Arizona 1912 as revised to January 1975

California

- Constitution of the State of California 1849 as amended

Delaware

- The Delaware Constitution of 1897 as amended (Delaware Code)

Florida

- Constitution of the State of Florida as revised in 1968 and amended to 1975

Georgia

- Constitution of the State of Georgia revised January 2005 (Georgia Code)

New York

- The Constitution of the State of New York as revised with amendments adopted and approved in 1938 and as amended and in force since January 1 2002

OTHER STATUTES

AUSTRALIA

- The (Commonwealth) Privacy Act 1988
- The Privacy Amendment Act 1990
- The Privacy Amendment (Private Sector) Act 2000

CANADA

- The Access to Information Act 1982
- The Privacy Act 1980
- The Personal Information Protection and Electronic Documents Act 2000

FRANCE

- French Data Protection Act 1978

GERMANY

- *Bundesdatenschutzgesetz* - Federal Data Protection Act 27 January 1977
- *Bürgerliches Gesetzbuch* - German Civil Code 1896 as amended by Act 25 June 1988
- *Kunsturhebergesetz* Law of Artistic Creations 1907
- *LuKDG*- Information and Communication Services (Multimedia) Act 1997- Federal Act Establishing the General Conditions for Information and Communication Services (German Multimedia Law) 13 June 1997
- *Gesetz über Personalausweise* (BGBl I, S. 548) 21 April 1986
- Telecommunications Carriers Data Protection Ordinance of 1996- (TDSV) 12 July 1996
- *Urheberrechtsgesetz*- German Copyright Law 9 September 1965

NEW ZEALAND

- The Ombudsman Act (1975)

NIGERIA

- Computer Security and Critical Information Infrastructure Protection Bill (2005)
- Copyright Act (Cap 68 LFN 1990) as amended by Copyright (Amendment) Decree (No 42 of 1999)
- Criminal Code Act (Cap 77 LFN 1990)
- Criminal Procedure Act (Cap 80 LFN 1990)
- Defamation Law 1961 (Cap 34 Laws of Lagos State 1973)
- Defamatory and Offensive Publications Act (Cap 93 LFN 1990)
- Evidence Act (Cap 112 LFN 1991) as amended by the Evidence (Amendment) Decree (No 62 of 1991)
- Income Tax (Authorized Communications) Act (Cap 175 LFN 1990)
- Interpretation Act (Cap 192 LFN 1990)
- Law Reform (Torts) Law 1961 (Cap 67 Laws of Lagos State 1973)
- National Population Commission Act (Cap 270 LFN 1990) as amended by National Population (Amendment) Decree (No 16 of 1999)
- Nigerian Communications Act (No 7 of 2003)

- Ondo State Edict (No 4 of 1989)
- Penal Code Act ((Northern States) Federal Provisions Act (Cap 345 LFN 1990)
- Public Health Act (Cap 65, 1958)
- Sharia Penal Code Law (Zamfara State of Nigeria Law No 10, 2000)
- Constitution (Suspension and Modification) Decree (No 1 of 1966)
- Constitution (Suspension and Modification) Decree (No 1 of 1984)
- State Security (Detention of Persons) (Amendment) (No2) Decree (No 24 of 1990)
- State Security and Detention of Persons Decree (No 2 of 1984)
- Telecommunications and Postal Offences Decree (No 21 of 1995) as amended by
Telecommunications and Postal Offences (Amendment) Decree (No 19 of 1997)
- Telegraphs Ordinance 1916
- Wireless Telegraphy Act (No 31 of 1961)
- Wireless Telegraphy Act 1990 as amended by the Wireless Telegraphy Amendment
Decree (No 31 1998)
- Wireless Telegraphy Ordinance [Cap 233, 1948 Revised Edition of the Laws of Nigeria]

SOUTH AFRICA

- Civil Proceedings Evidence Act No 25 of 1965 as amended by Evidence Law
- Companies Act No 61 of 1973
- Consumer Protection Bill 2007
- Copyright Act No 98 of 1978
- Criminal Procedure Act 51 of 1977 as amended by Criminal Procedure (Second)
Amendment Act No 62 of 2001
- Electronic Communications and Transactions Act No 25 of 2002
- Identity Act No 68 of 1977 as amended by Identity Amendment Act No 28 of 2000
- Income Tax Act 58 of 1962 as amended by Act No 19 of 2001
- Indecent or Obscene Photographic Matter Act No 37 of 1967
- Interception and Monitoring Bill August 2001 [B50-2001]
- Interception and Monitoring (Prohibition) Act No 127 of 1992

- Interception and Monitoring (Prohibition) Amendment Act No 77 of 1995
- Internal Security Act No 74 of 1982
- Medicines and Related Substances Control Act No 101 of 1965
- Natal Law to Amend the Law of Evidence (Evidence Law No 5 of 1870)
- National Credit Act No 34 of 2005
- Open Democracy Bill 1998 [B67-1998]
- Powers and Privileges of Parliament Act No 91 of 1963
- Powers and Privileges of Provincial Councils Act No16 of 1948
- Promotion of Access to Information Act No 2 of 2000 as amended by Access to Information Amendment Act No 54 of 2002
- Recognition of Customary Marriages Act No 120 of 1998
- Statistics Act 66 of 1976 as amended by No 6 of 1999
- Telecommunications Act No 103 of 1996 as amended by Telecommunications Amendment Act No 64 of 2001
- Telegraph Messages Protection Act No 44 of 1963

UNITED KINGDOM

- Access to Health Records Act 1990 (Chapter 23)
- Access to Health Records (Control of Access Regulations) 1993 (SI1993/746)
- Access to Medical Reports Act 1988 (Chapter 28)
- Adoption Act 1976 (Chapter 36)
- Broadcasting Act 1990 (Chapter 42)
- Children Act 1989 (Chapter 41)
- Children and Young Persons Act 1933 (23 & 24 Geo.5) (Chapter 12)
- Consumer Credit Act 1974
- Copyrights Designs and Patents Act 1998 (Chapter 48)
- Criminal Justice Act 1988 (Chapter 33)
- Data Protection Act 1984 (Chapter 35)
- Data Protection Act 1998 (Chapter 29)
- Defamation Act 1952 (Chapter 66)

- Defamation Act 1996 (Chapter 31)
- Human Rights Act 1998 (Chapter 42)
- Interception of Communications Act 1985 (Chapter 56)
- Magistrates' Courts Act 1980 (Chapter 43)
- Official Secrets Act 1989 (Chapter 6)
- Police Act 1997 (Chapter 50)
- Post Office (Data Processing Services) Act 1967
- Protection from Harassment Act 1997 (Chapter 40)
- Rehabilitation of Offenders Act 1974 (Chapter 53)
- Sexual Offences (Amendment) Act 1976 (Chapter 82)
- Sexual Offences (Amendment) Act 1991 (Chapter 31)
- Telecommunications Act 1984 (Chapter 12)
- Theatres Act 1968 (Chapter 54)

UNITED STATES OF AMERICA

- Alabama Code
- Alaska Stat.
- Arizona Rev. Stat.
- Arkansas Stat. Ann.
- California Civil Code
- Children's Online Privacy Protection Act 1990 (15 USC Ss 6501-6506)
- Computer Matching and Privacy Protection Act 1988 (5 USC S 552a) (PI 101-56, 1989)
- Communications Decency Act (Title V of the Telecommunications Act) 1996 PI No 104-104, Sec.502, 110 Stat. 56, 133-35
- Drivers Privacy Protection Act 1994 (18 USC S 2721)
- Electronic Communications Privacy Act (18 USC S 2510)
- Electronic Freedom of Information Act 1986 (5 USC S 552)
- Electronic Funds Transfer Act 1978 (15 USC Ss 1693-1693r)
- Fair Credit Reporting Act 1970 (15 USC S 1618) as amended
- Family Educational Rights and Privacy Act 1974 (20 USC S 1232g)

- Federal Copyright Law (17 USC S 101)
- Freedom of Information Act 1966 (5 USC S 552) as amended
- Illinois Rev. Stat. Ann. Ch 161 (Supp.1977)
- Maine Rev. Stat.
- Maryland Ann. Code Art. 11
- Michigan Comps. Laws Ann.
- Mont. Rev. Codes Ann.
- New Hampshire Rev. Stat. Ann.
- Privacy Act 1974 (5 USC S 552a) as amended
- Restatement of the Law (Second) Torts Subsection 652 (1997)
- Restatement of the Law (3rd) Unfair Competition Subsection 47 (1995)
- Restatement of Torts Subsection 757 (1939)
- Right to Financial Privacy Act 1978 (12 USC S 3401)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001 (PL107-56; 115 Stat.272 2001)
- Utah Code Ann.
- Video Privacy Protection Act 1988 (18 USC S 2710)
- Wiretap Act 1968 (Title 3 of the Omnibus Crime Control and Safe Streets Act) 18 USC S 2511

CONVENTIONS, DIRECTIVES, DECLARATIONS, GUIDELINES

- Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data ETS No 108, 1981

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
- Organisation for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data 1981
- United Nations International Convention on Civil and Political Rights 1966
- Universal Declaration of Human Rights 1948

TABLE OF CASES

EUROPEAN UNION

- *ADT v United Kingdom* (2000) 37 ECHR
- *B v France* (1992) 16 EHRR 1
- *Buckley v United Kingdom* (1994) 18 EHRR 191
- *Christie v United Kingdom* (1994) 78-A DR 119
- *Cossey v United Kingdom* (1990) 13 EHRR 622
- *Dudgeon v United Kingdom* (1981) 4 EHRR 149
- *Earl Spencer v United Kingdom* (1998) 92 DR 56
- *Gillow v United Kingdom* (1986) 11 EHRR 335
- *Golder v United Kingdom* (1975) 1 EHRR 54
- *Halford v United Kingdom* (1997) 24 EHRR 253
- *Klass and others v Germany* (1978) 2 EHRR 214
- *Laskey, Jaggard & Brown v United Kingdom* (1997) 24 EHRR 39
- *Malone v United Kingdom* (1984) 7 EHRR 14
- *Marckx v Belgium* (1979) 2 EHRR 330
- *Niemetz v Germany* (1992) 16 EHRR 97
- *Rees v United Kingdom* (1986) 9 EHRR 56
- *Smith & Grady v United Kingdom* (2000) 29 EHRR 493
- *Sunday Times v United Kingdom* (1979-80) 2 EHRR 245
- *Whiteside v United Kingdom* (1994) 18 EHRR CD 126
- *Winer v United Kingdom* (1986) 48 DR 154
- *X and Y v The Netherlands* (1986) 8 EHRR 235
- *X v United Kingdom* (1997) 24 EHRR 143

FRANCE

- *Rachel affaire* Judgement of June 16, 1858, Trib. Pr. Inst. De la Seine, 1858 D.P. 111

GERMANY

- *BGH 20, 1 (1965) Gretna Green case*
- *BGH 9, 5 (1985); 1986 IIC 681 Inkasso-Programm case*
- *BGH 4, 10 (1990); 1991 IIC 723 Betriebssystem case*
- *BGH 9,11 (1993); BGHZ 52, 124*
- *BGH 15, 11 (1994); BGHZ 128, 1; NJW 861 (1995) Princess Caroline of Monaco*

- *13 BGHZ 334 (1954) Schacht case*
- *15 BGHZ 249 (1954) Cosima Wagner case*
- *20 BGHZ 345 (1956) Paul Dahlke case*
- *26 BGHZ 249 (1958) Herrenreiter case*
- *35 BGHZ 363 (1961); NJW 2059 (1961) Ginseng-Wurzel case*

- *1 BVerfGE 27; NJW 1707 (1969)*
- *1 BVerfGE 65 (1941)*
- *27 BVerfGE 1 (1969) Microcensus case*
- *27 BVerfGE 344; NJW 555-6 (1970) Divorce Records case*
- *30 BVerfGE 1 (1970) Klass case*
- *30 BVerfGE 1 (1970) "Monitoring" Opinion*
- *30 BVerfGE 173 (1971)*
- *32 BVerfGE 54 (1971) Dry Cleaning case*
- *32 BVerfGE 373 (1972) Medical Confidentiality case*
- *34 BVerfGE 238 (1973)*
- *34 BVerfGE 269 (1973) Princess Soraya case*
- *35 BVerfGE 35 (1973) Klaus K. case*
- *35 BVerfGE 202 (1973)*
- *35 BVerfGE 311 (1973) Prison Correspondence II case*
- *39 BVerfGE 1 (1975) Abortion I case*
- *42 BVerfGE 212 (1976) Bauer Company case*
- *51 BVerfGE 97 (1978)*
- *54 BVerfGE 208 (1980) Boll case*

- 59 BVerfGE 95 (1982)
- 65 BVerfGE 1 (1983)
- 67 BVerfGE 157 (1985)
- 75 BVerfGE 318 (1986)
- 77 BVerfGE 1(1987)
- 78 BVerfGE 77 (1988)
- 85 BVerfGE 386 (1992) *Connection Capture case*
- 88 BVerfGE 203 (1993) *Abortion II case*
- 101 BVerfGE 361 (1999)

- 69 RGZ 404 (1908)
- 115 RGZ 416 (1927)

GHANA

- *Aubin v Ehunaku* [1960] GLR 167
- *Inneh v Aruegbon* (1952) 14 WACA 73
- *Mansour v El Nasr Export and Import Co* [1963] 2 GLR 316
- *Soadwah v Obeng* [1966] GLR 33

NIGERIA

- *Abiola v Ijoma* [1970] 2 All NLR 268
- *Bakare v Oluwide* [1969] 2 All NLR 324
- *Balogun v Alakija* [1963] 2 All NLR 75
- *Bankole v Admekwe* (1973) 12 CCHCJ 97
- *Dabira v Adelaja* (1973) 11 CCHCJ 97
- *De facto Works Ltd v Odumotun Trading Co Ltd* [1959] LLR 33
- *Gloria Mowarin v Attorney -General of the Federation* (Unreported) The Guardian Feb 20 1991
- *Karunwi v Wema Bank Ltd* [1977] 3 CCHCJ 61
- *Lakanmi v Attorney -General of the Western State & others* (1971) UILR 20
- *Mutual Aid Society Ltd v Akerele* [1966] NMLR 257

- *Niger Chemists Ltd v Nigeria Chemists* [1961] 1 All NLR 171
- *Nwankwa v Ajaegbu* (1978) 2 LRN 230
- *Ogunlende v Babayemi* (1971) 1 UILR 417
- *R v Holmes* (1871) L.R. ICCR 334
- *Tebite v Nigeria Marine & Trading Co Ltd* (1971) 1 UILR 432
- *Theophilus Awobokun v The Sketch Publishing Coy Ltd & others* (1973) 3 UILR 502
- *The Queen v Bartholomew Princewell* [1963] 2 All NLR 31
- *Tony Momoh v Senate* (1981) NCLR 105
- *UK Tobacco Co Ltd v Carreras Ltd* [1931] 16 NLR 1

SOUTH AFRICA

- *AAIL (SA) v Muslim Judicial Council* (Cape) 1983 (4) SA 855 (C)
- *A Neuman v Beauty Without Cruelty International* 1986 (4) SA 675 (C)
- *Bernstein v Bester (NO)* 1996 (2) SA 751(CC)
- *Boka Enterprises (Pvt) Ltd v Manatse* 1990 (3) SA 626 (ZH)
- *Boswell v Union Club of SA (Durban)* 1985 (2) SA 162 (D)
- *C v Minister of Correctional Services* 1996 4 SA 292 (T)
- *Carmichelle V Minister of Safety and Security (Centre for Applied Legal Studies Intervening)* 2001 4 SA 938 (CC)
- *Case & Another v Minister of Safety & Security* 1996 (3) SA 617 (CC)
- *CCII Systems (Pty) Ltd v Fakie NNO* 2003 (2) SA 325 (T)
- *Church of Scientology in South Africa Incorporated Association not for Gain v Readers Digest Association (SA) (Pty) Ltd* 1980 (4) SA 313 (C)
- *Coetzee v Nel* 1972 (1) SA 353 (A)
- *Combrinck v De Kock* 1887 (5) SC 405
- *Dantex Investment Holdings (Pty) Ltd v Brenner* 1989 (1) SA 390 (A)
- *Davis v Additional Magistrate, Johannesburg, & Others* 1989 (4) SA 299 (W)
- *De Fourd v Council of Cape Town* (1898) 15 SC 399
- *Dhlomo (NO) v Natal Newspapers (Pty) Ltd & Another* 1989 (1) SA 945 (A)

- *Epstein v Epstein* 1906 TH 87
- *Estate Dempers v Secretary for Inland Revenue* 1977 (3) SA 410 (AD)
- *Fedics v Matus* 1997 (BCLR) 1199 (C)
- *Ferela (Pty) Ltd & Ors v Commissioner for Inland Revenue & Ors* 1998 (4) SA 275 (T)
- *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A)
- *GA Fichardt Ltd v The Friend Newspapers Ltd* 1916 (AD)
- *Gardener v Whitaker* 1995 (2) SA 672 (E); 1994 (5) BCLR 19 (E)
- *Geyser en 'n ander v Pont* 1968 (4) SA 67 (W)
- *Goodman v Von Moltke* 1938 CPD 153
- *Gosschalk v Rossouw* 1996 (2) SA 476 (C)
- *Grütter v Lombard* 2007 (4) SA 89 (SCA), (3) All SA 311 (SCA)
- *Hearson v Natal Witness Ltd* 1935 NPD 603
- *Holomisa v Argus Newspapers Ltd* 1996 (2) SA 588 (W)
- *Hyundai Motor Distributors (Pty) Ltd & Ors v Smit NO & ors* 2000 (2) SA 934 (T)
- *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A)
- *Jansen van Vuuren & Another NNO v Kruger* 1993 (4) SA 842 (A)
- *Jeeva v Receiver of Revenue Port Elizabeth* 1995 (2) SA 433 (SECLD)
- *Johnson v Beckett* 1992 (1) SA 762 (A)
- *Jooste v National Media Ltd* 1994 (2) SA 634 (C)
- *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (T)
- *King v Dykes* 1971 (3) SA 540
- *Klein v Attorney- General WLD & Another* 1995 (3) SA 848 (W)
- *Knoeson v Theron* 1904 (21) SC 177
- *Lappan v Corporation of Grahamstown* 1906 EDL 41
- *Lebowa en 'n Ander v De Meyer NO* 1993 (4) SA 13 (A)
- *Lenco Holdings Ltd v Eckstein* 1996 (2) SA 693 (N)
- *Maisel v Van Naeren* 1960 (4) SA 836 (C)
- *Mandela v Falati* 1995 (1) SA 257 (W)
- *Mangaroo v Toolsee* (1927) 48 NLR 100
- *Marais v Richard* 1981 (1) SA 1157 (A)

- *Mhlongo v Bailey & Another* 1958 (1) SA 370 (W)
- *Minister of Justice v Hofmeyr* 1993 (3) SA 131 (A)
- *Mistry v Interim National Medical and Dental Council of South Africa & Others* 1998 (7) BCLR 880 (CC)
- *Muller v SA Associated Newspapers Ltd* 1972 (2) SA 589 (C)
- *Multiplan Insurance Brokers (Pty) Ltd v Van Blerk* 1985 (3) SA 164 (D)
- *National Coalition for Gay and Lesbian Equality & Others v Minister of Justice & Others* 1998 (6) BCLR 726 (W), (2) SACR 102 (W)
- *National Media Ltd & Another v Jooste* 1996 (3) SA 262 (A)
- *National Media Ltd v Bogoshi* 1998 (4) SA 1195 (SCA)
- *Nel v Le Roux & Others* 1996 (3) SA 562 (CC)
- *Nell v Nell* 1990 (3) SA 889 (T)
- *O'Keefe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C)
- *Pickard v SA Trade Protection Society* (1905) 22 SC 89
- *R v Daniels* 1938 TPD 312
- *R v Diedericks* 1957 (3) SA 661 (E)
- *R v Ferreira* (1943) NPD 19
- *R v Holliday* 1927 CPD 395
- *R v Jungman* 1914 TPD 8
- *R v Schoonberg* 1926 OPD 247
- *R v Umfaam* 1908 TS 62
- *R v Van Meer* 1923 OPD 77
- *Reid-Daly v Hickmann & Others* 1981 (2) SA 315 (ZA)
- *Rhodes University College v Field* 1947 (3) SA 437 (A)
- *Rhodesian Printing and Publishing Co Ltd v Duggan & Another* 1975 (1) SA 590 (RA)
- *S v A and Another* 1971 (2) SA 293 (T)
- *S v Boshoff & Others* 1981 (1) SA 393 (T)
- *S v Bosman* 1980 (1) SA 852
- *S v Dube* 2000 (2) SA 583 (N)
- *S v Gumede & Another* 1998 (5) BCLR 530 (D)
- *S v Hammer & Others* 1994 (2) SACR 496 (C)

- *S v Heyman* 1966 (4) SA 598 (A)
- *S v Human & Another* 1996 (1) SA 232 (W)
- *S v I and Another* 1976 (1) SA 781 (RA)
- *S v Kidson* 1999 (1) SACR 338 (W)
- *S v Kleinschmidt* 1980 (1) SA 852
- *S v Lwane* 1966 (2) SA 433 (A)
- *S v Madiba & Another* 1998 (1) BCLR 38 (D)
- *S v Manamela* 2000 (1) SACR 414 (CC)
- *S v Motloutsi* 1996 (1) SA 584 (CC), 1996 (2) BCLR 220 (CC)
- *S v Naidoo & Another* 1998 (1) BCLR 46 (N), 1998 (1) SACR 478 (N)
- *S v Naude* 1975 (1) SA 681 (A)
- *S v Nkabinde* 1998 (8) BCLR 996 (N)
- *S v Zwayi* 1998 (2) BCLR 242 (CK)
- *Sackstein v South African Revenue Service* 2000 (2) SA 250 (SE)
- *Sather v Orr* 1938 AD 426
- *Sauk v O'Malley* 1977 (3) SA 394 (A)
- *Stellenbosch Wine Trust Ltd v Oude Meester Group Ltd* 1972 (3) SA 152 (C)
- *Thomas v Thomas* 1949 (1) SA 445 (A)
- *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T),
1979 (1) SA 441 (A)
- *Van Leggelo v Argus Printing & Publishing Co Ltd* 1935 TPD 230
- *Waring & Gillow Ltd v Sherborne* 1904 TS 340
- *Welz v Hall* 1996 (4) SA 1073 (C)
- *Wilhelm v Beamish* (1894) 11 SC 13

UNITED KINGDOM

- *Av B Plc* [2001] 1 WLR 2341; [2003] QB 195
- *AB v CD* [1851] 14 Dunlop 177
- *Albert v Strange* [1849] 2 De G & Sm 652, 64 ER 293 Ch
- *Allan v Liverpool Overseers* [1874] LR 9 QB 180

- *Anchor Brewhouse Developments v Berkeley House (Docklands Developments)* [1987] Ch D 2 EGLR [1978] 38 BLR 82
- *Angel v Bushell Ltd* [1968] 1 QB 813
- *Archbold v Sweet* [1832] 5 C7 P 219
- *Argyll v Argyll* [1965] 1 All ER 611, [1967] Ch 308
- *Attersoll v Stevens* [1808] 1 Taunt 183
- *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109
- *Barrymore v Newsgroup Newspapers Ltd* [1977] FSR 600
- *Becke v Smith* (1836) 2 M&W 195
- *Bernstein [of Leigh (Baron)] v Skyways & General Ltd* [1978] QB 479
- *Blackshaw v Lord* [1984] 1 QB 1
- *Bloodworth v Gray* [1844] 7 Man & G 334
- *Boardman v Phipps* [1967] 2 AC 46
- *Bone v Seale* [1975] 1 WLR 797
- *Bonnard v Perryman* [1891] 2 Ch 269
- *British Celanese Ltd v AH Hunt Capacitors Ltd* [1969] 1 WLR 959
- *Burnett v George* [1992] 1 FLR 156
- *Byrne v Deane* [1937] 1 KB 818
- *Campbell v MGN Ltd* [2003] QB 633
- *Cassidy v Daily Mirror Newspapers Ltd* [1929] 2 KB 331
- *Christie v Davey* [1893] 1 Ch 316
- *Commission of Taxation v United Aircraft Corporation* [1943-1944] 68 CLR 525
- *Cookson v Harewood* [1932] 2 KB 488n; 101 LJKB 394n
- *Cunard v Antifyre Ltd* [1933] 1 KB 551
- *Douglas v Hello! Ltd* [2001] QB 967; [2002] 1 FCR 289; 2003 EWHC 786
- *Exchange Telegraph Co v Howard* [1906] 22 TLR 375
- *Federal Commission of Taxation v United Aircraft Corporation* [1943-1944] 68 CLR 525
- *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892
- *Fraser v Thames Television Ltd* [1984] QB 44
- *Gabbitas v Gabbitas* The Times December 5, 1997

- *Gartside v Outram* [1857] 26 LJNS Ch
- *Godfrey v Demon Internet Ltd* [1999] 4 All ER 342
- *Granada Group Ltd v Ford Motor Co Ltd* [1972] FSR 103
- *Gray v Jones* [1939] 1 All ER 795
- *Grey v. Pearson* (1857) 6 HL CAS 61
- *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804
- *Hendriks v Montagu* [1881] 50 LJ Ch 456
- *Herbage v Pressdram Ltd* [1984] 1 WLR 1160; 128 SJ 615; [1984] 2 All ER 769
- *Herbert Morris Ltd v Saxelby* [1916] 1 AC 688
- *Hines v Winnick* [1974] Ch 708
- *Hird v Wood* [1894] 38 Sol J 234
- *Hollywood Silver Fox Farm Ltd v Emmet* [1936] 1 All ER 825
- *Houseman v Coulson* [1948] 2 DLR 62
- *Hunter v Canary Wharf Ltd* [1997] AC 655
- *Hunter v Mann* [1974] 1 QB 767
- *Huth v Huth* [1915] 3 KB 32
- *Initial Services v Putterhill* [1968] 1 QB 396
- *Janvier v Sweeney* [1919] 2 KB 316
- *Jeffries v Duncombe* (1809) 11 East 227
- *John v MGN Ltd* [1997] QB 586
- *Joyce v Sengupta* [1993] 1 All ER 897 (CA)
- *Kaye v Robertson* [1991] FSR 62
- *Khasoggi v Smith* [1980] 124 SJ 149 (CA)
- *Khorasandjian v Bush* [1993] QB 727 (CA)
- *King v Lake* [1667] 1 Hardres 470
- *Lennon v News Group Newspapers and Twist* [1978] FSR 573 (HL)
- *Lion Laboratories v Evans* [1985] 1 QB 526; [1984] 3 WLR 539
- *Lord Ashburton v Pape* [1913] 2 Ch 469
- *Lord Bryon v Johnston* [1816] 35 ER 851
- *Loutchansky v Times Newspapers Ltd (No 2)* [2002] QB 783
- *Malone v Laskey* [1907] 2 KB 141

- *Malone v Metropolitan Police Commissioner* [1979] Ch 344; [1979] 2 All ER 620
- *McCarey v Associated Newspapers (No 2)* [1965] 2 QB 86
- *McLoughlin v O'Brian* [1983] 1 AC 410
- *McManus v Beckham* [2002] 1 WLR 2982
- *Millar v Taylor* [1769] 98 ER 201
- *Minter v Priest* [1930] AC 558
- *Monson v Tussauds Ltd* [1894] 1 QB 671
- *Morison v Moat* [1851] 9 Hare 241
- *Mrs R v Central Television Plc* [1994] Fam 192
- *Oldham v Lawson* [1976] VR 654
- *Owen and Smith v Reo Motors (Britain) Ltd* [1934] 151 LT 271
- *Parmiter v Coupland* [1840] 6 M 7 W 105
- *Pollard v Photographic Co* [1889] 40 Ch D 845
- *Prince Jefri Bolkiah v KPMG* [1999] 1 All ER 577
- *Protea Technology Ltd & anor v Wainer & ors* 1997 (3) SA 694
- *R v Brent London Borough Council, Ex p Peck* TLR 18 December 1997
- *R v Keeton* [1970] 54 Cr App 267
- *R v Khan* [1997] AC 558
- *R v Masqud Ali* [1966] 1 QB 688
- *R v Sang* [1979] 3 WLR 263
- *R v Senat* [1968] 52 Cr App R 282
- *Read v J Lyons & Co Ltd* [1947] AC 156
- *Reckitt & Colman (Products) Ltd v Borden Inc* [1990] 1 WLR 491 (HL)
- *Ridge v The Illustrated English Magazine* [1913] 29 TLR 592
- *Robb v Green* [1895] 2 QB 1
- *Rolls Royce Ltd v Jeffrey* [1962] 1 All ER 801
- *Saltman Engineering v Campbell Engineering* [1948] 65 RPC 203
- *SCM (UK) Ltd v Whittall & Sons Ltd* [1970] 2 All ER 417
- *Seager v Copydex* [1967] RPC 349, [1967] 1 WLR 923
- *Sheen v Clegg* (1961) Daily Telegraph June 22
- *Shelley Films v Rex Features* [1994] EMLR 134

- *Sim v Heinz* [1959] 1 All ER 547
- *Sim v Stretch* (1936) 52 TLR 669
- *Slipper v British Broadcasting Corporation* [1991] 1 QB 283
- *Spicer v Smee* [1946] 1 All ER 489
- *Sports and General Press Agency Ltd v "Our Dogs" Publishing Co* [1917] 2 KB 125

(CA)

- *Stephens v Avery* [1988] 1 Ch 449
- *Sutcliffe v Pressdram Ltd* [1990] 1 All ER 269
- *Sutherlands v Stopes* [1925] AC 47
- *Technograph Printed Circuits Ltd v Chahoyne* [1967] RPC 399
- *Terrapin v Builders' Supply Co (Hayes) Ltd* [1967] RPC 375
- *Theaker v Richardson* [1962] 1 WLR 151
- *Thompson v Ward* [1953] 2 QB 153
- *Tolley v J S Fry & Sons Ltd* [1931] AC 333
- *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461
- *Venables v News Group Newspapers Ltd* [2001] Fam 430
- *Vernon v Bosley* [1977] 1 All ER 577
- *Walter v Alltools Ltd* [1944] 61 TLR 39
- *Wilkinson v Downton* [1897] 2 QB 57
- *Williams v Reason* [1988] 1 WLR 96
- *Woodward v Hutchins* [1977] 2 All ER 751
- *X v Y* [1988] 2 All ER 648
- *X Ltd v Morgan Grampian (Publishers) Ltd* [1991] 1 AC 1
- *Youssouf v Metro-Goldwyn-Mayer Pictures Ltd* [1934] 50 TLR 581

UNITED STATES OF AMERICA

- *Alana Shoars v Epson America, Inc.* (1990) (No B 073234) LaSC
- *Avrahami v US News & World Report* (CCA, Virginia, 1996) (No 95- 1318)
- *Bartnicki v Vopper* (2001) 532 US 514, 121 S Ct 1753
- *Bechhoefer v U.S. Dept of Justice Drug Enforcement Admin* 209 F 3d 57 (2d Cir 2000)

- *Bowers v Hardwick* (1986) 478 US 186, L Ed 2d 140, 146, 106 SCt 2481
- *Boyd v U.S.* (1896) 116 US 616
- *California Bankers Association v Schultz* (1974) 416 US 21
- *Cape Pubs Inc v Bridges* (1982) 423 So 2d 426 (Fla App)
- *Carson v Here's Johnny Portable Toilets Inc.* 698 F2d 831 (6th Cir 1983)
- *Chrysler Corporation v Brown* (1979) 99 S.Ct. 1795
- *Cobey v State* (1989) 80 Md App 31, 559 A 2d 3al (md) App
- *Connecticut Nat'l Bank v. Germain* (1992) 112 S.Ct. 1146, 1149
- *Critical Mass Energy Project v NRC* 975 F 2d 871 (Dc Cir. 1992); (1993) 113 S Ct 1579
- *Davis et al v Gracey et al* No 85-6245 (10th Cir. 21 April 1997)
- *Delaraba v Nassau County Police Dept* (1994) 83 NY2d 367, 610 NY2d 928, 632vNE2d 1251, 9 BNA IER Cas 467
- *Dempsey v National Enquirer*(D.Me.1989) 702 F.Supp.934
- *Department of Justice v Reporters Committee for Freedom of the Press* (1989) 489 US 749
- *Dietemann v Time Inc* 449 F2d 245 (9th Cir 1971)
- *Ditman v California*191 F3d 804 (9th Cir 1999)
- *Doe v United States Air Force* 812 F 2d 738 (DC Cir 1987)
- *Dresser Industries v United States* 596 F.2d 1231 (5th Cir 1979)
- *Edison v Dept of the Army* 672 F 2d 840 (11th Cir. 1982).
- *Factors Etc.Inc.v Pro Arts Inc.* 579 F 2d 215 (2nd Cir1978)
- *Galella v Onassis* 487 F.2d 986 (2d Cir 1973)
- *Goodyear Tire & Rubber Co v Vandergriff* (1936)52 Ga App 662
- *Graham v Hawk* (6th Cir 1995) 857 F Supp 38 (WD Tenn 1994); 59 F 3d 170
- *Griswold v Connecticut* (1965) 381 US 479
- *Hill v National Collegiate Athletic Association*1 Cal App 4th 1398 (1990 6th Dist)
- *Hirsch v S.C. Johnson & Sons Inc.* (1979) 90 Wis. 2d 379, 280 NW2d
- *James v Douglas* 941 F2d 1529 (1991 Ca 11 Ga)
- *Jones v United States Dept of Treasury* (DDC Oct 18, 1983) (No. 82- 2420); 744 F 2d 878 (DC Cir 1984)

- *Katz v United States* (1967) 389 US 347
- *Kyllo v United States* (2001) 533 US 27, 121 S Ct 2038
- *Lawrence v State of Texas* (2003) 539 US 558
- *Leckelt v Board of Commissioners of Hospital* (1990) CA 5 LA 909 F2d 820, 53 BNA FEP Cas 1136
- *Lopez v United States* (1963) 373 US
- *Loving v Virginia* (1967) 388 US 1, 18 L Ed 2 d 1010, 87 S Ct 1817
- *Maroscia v Levy* 569 F.2d 100 (7th Cir 1977)
- *McGregor v Greer* 748 F Supp 881 (DDC1990)
- *McIntire v Ohio Elections Committee* (1995) 115 US 1511
- *Mcnamara v Freedom Newspapers* (1991) Tex App Corpus Christi 802 SW 2d 901
- *McVeigh v Cohen et al* (DDC 1998) 983 F Supp 215
- *Menard v Mitchell* 430 F.2d 486 (DC Cir 1970)
- *Midler v Young & Rubicam* 849 F2d 460 (9th Cir1988)
- *Miller v Motorola* (1990) III App Ct; 560 NE 2d 900
- *Miranda v Arizona* (1966) 384 US 436
- *Moore v East Cleveland* (1977) 431 US 494, 52 L Ed 2d 531, 97 S Ct 1932
- *Motschenbacher v R.J. Reynolds Tobacco Co.* 498 F2d 821 (9th Cir 1974)
- *Muller v. BP Exploration (Alaska) Inc.* (1996) 923 P.2d 783
- *Murray v Schlosser* (1990) 574 A.2d 1339
- *NAACP v Alabama*(1958) 387 US 449
- *National Federation of Fed. Employees v Greenberg* 789 F Supp 430 (DDC 1992)
- *New Jersey v T.L.O.* (1985) 469 US 325
- *New York Times v Sullivan* (1964) 376 US 254
- *Nixon v A.G. Administrator of General Services* (1970) 433 US 425
- *N.L.R.B. v Robbins Tire & Rubber Co.* (1978) 98 S.Ct. 2311
- *O'Connor v Ortega*(1987) 480 US 709
- *Onassis v Christian Dior – New York Inc* (1984) 472 NYS 2d 254
- *Parks v IRS* 618 F 2d 677 (10th Cir. 1980)
- *Pavesich v New England Life Insurance Co.* (1905)122 Ga.190, 50 SE 68
- *People v Castro* (1989) 144 Misc 2d 956, 545 NYS2d 985 S Ct

- *People v Shinkle* (1989)128 III 2d 480, 132 III Dec 432, 539 NE2d 1238
- *Perez-Santos v Malave* 23 Fed App 11 (1st Cir 2001)
- *Petroleum Info Corp v U.S. Dept of Int* (1992) 976 F 2d 1429
- *Pilon v U.S. Dept of Justice* 73 F3d 1117-1124 (DC Cir 1996)
- *Planned Parenthood of Southeastern Pennsylvania v Casey* (1992)112 S Ct 931, 112 S Ct 2791
- *Quarles v Dept of Justice* (1990) 890 F2d 390
- *Quinn v Stone* 978 F 2d 126 (3rd Cir. 1992)
- *Rakas v Illinois*
- *Raven v Panama Canal Co* 583 F2d 169 (5th Cir 1978)
- *Re L.A.* (Kan 2001) 21P. 3d 952, 961
- *Recticel Foam Corp v U.S. Dept of Justice* (No 98-2523) (DDC Jan 31, 2002)
- *Reinbold v Evers* 187 F 3d 348 (4th Cir 1999)
- *Reno v American Civil Liberties Union* (1997) 117 S Ct 2329
- *Reno v Condon* (2000) 528 US 141
- *Roe v Wade* (1973) 410 US 113, 93 S Ct 705
- *Ross v Midwest Communications Inc.* (1989) CA 5 Tex 870 F2d 271, 16, Media LR 1463
- *Sable Communications of California Inc v FCC* (1989) 492 US 115
- *Silverman v United States* (1961) 365 US 505
- *Smith v Maryland* (1979) 442 US 735, 61 L Ed 2d 220, 99 S Ct 2577
- *Soroka v Dayton Hudson Corp.* (App 1991)1 Cal Rep 2d 77, 6 IER Cases (BNA) 1491
- *St Michael's Convalescent Hospital v California* (9th Cir 1981) 643 F.2d, 1369, 1373
- *Steve Jackson Games Inc. v US Secret Service* (5th Cir 1994) 816 F Supp 432 (W.D. Tex 1993); 36F 3d 457
- *Sutton v Providence St Joseph Medical Centre* 192 F3d 826 (9th Cir 1999)
- *The Florida Star v BJJF* (1989) 491 US 524, 536-7
- *Tobey v NLRB* (DC Cir 1994) 40 F3d 469
- *United States v Bressler* 772 F 2d 287(7th Cir 1985)
- *United States v David Lee Smith* (1992) 978 F2d 171 US App
- *United States Dept of Justice v Landano* (1993) 113 S Ct 2014

- *United States v Gonzales* (No 76-132) (MD La Dec 21, 1976)
- *United States v Karo* (1984) 468 US 705
- *United States v Little* (1971) 321F Supp 388 D Del
- *United States v Miller* (1976) 425 US 435
- *United States V Morton Salt Co* (1950) 338 US 632
- *United States v Trabbert* 978 F Supp 1368 (D Colo 1997)
- *UNT v Aerospace Corp* (9th Cir 1985) 765 F2d 1440
- *Wanbun Inini v Sessions* 900 F 2d 1234 (8th Cir. 1990)
- *Watchtower Bible & Tract Society of N.Y. v Village of Stratton* (2002)
122 S.Ct 2080
- *Waters v Thornburgh* 888 F 2d 870 (DC Cir 1989)
- *Webb v Magaw* 880 F Supp 20 (DDC 1995)
- *Whalen v Roe* (1977) 429 US 589
- *White v Samsung Electronics America Inc* 989 F2d 1512 (9th Cir 1993)
- *Wine Hobby v I. R. S.* 502 F.2d 133 (3d Cir 1974)
- *Wolfe v HHS* (1988) 839 F 2d 768
- *Zeran v America Online* 129 F 3d 327 (4th Cir 1997)