

2011

Privacy protection in the information and communications technology (ICT): a comparative analysis of the laws of the United States, European Union and Jordan

Akram Almatarneh

University of Wollongong, akram@uow.edu.au

Recommended Citation

Almatarneh, Akram, Privacy protection in the information and communications technology (ICT): a comparative analysis of the laws of the United States, European Union and Jordan, Doctor of Philosophy thesis, Faculty of Law, University of Wollongong, 2011.
<http://ro.uow.edu.au/theses/3470>

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

**Privacy Protection in the Information and
Communications Technology (ICT):** *A
Comparative Analysis of the Laws of the United States, European
Union and Jordan*

**A Thesis Submitted in Fulfilment of the Requirements for the Award of the Degree
of**

Doctor of Philosophy

From

University of Wollongong

By

Akram Almatarneh

LL.B (MU, Jordan) LL.M (UWS, Australia) M.Phil (Macquarie University, Australia)

Faculty of Law

2011

SUMMARY OF CONTENTS

CONTENTS.....	ii
LIST of FIGURES, TABLES and APPENDICES.....	viii
ABBREVIATIONS.....	ix
ACKNOWLEDGMENTS.....	xi
STATEMENT OF AUTHORSHIP.....	xiii
AUTHOR'S PUBLICATIONS.....	xiv
ABSTRACT.....	xv
CHAPTERS 1–9.....	1
BIBLIOGRAPHY.....	447
APPENDICES.....	478

CONTENTS

Chapter One

General Introduction

1.1 Background to the Research.....	1
1.2 Statement of the Problem.....	3
1.3 Research Questions.....	8
1.4 Conceptual Framework.....	9
1.5 Aims and Objectives of the Research.....	17
1.6 Approach and Methodology.....	19
1.7 Literature Review.....	22
1.8 Chapter Outline.....	33

Chapter Two

The Concept of Privacy

2.1 Introduction.....	38
2.2 Definition of Privacy.....	39
2.3 Importance of Privacy.....	46
2.4 Privacy as a Legal Concept: Property Right or Human Right?.....	56
2.5 Privacy and Other Concepts.....	62
2.5.1 Privacy and Secrecy.....	62
2.5.2 Privacy and Confidentiality.....	64
2.5.3 Privacy and Reputation.....	66
2.5.4 Privacy and Security.....	67
2.6 International Recognition of the Right to Privacy.....	68
2.6.1 Universal Declaration on Human Rights (UDHR (1948), Article 12).....	69
2.6.2 International Covenant on Civil and Political Rights (ICCPR (1976), Article 17).....	70
2.6.3 European Convention on Human Rights (ECHR (1950), Article 8).....	72
2.6.4 American Convention on Human Rights (ACHR (1969), Article 11).....	75
2.6.5 Cairo Declaration on Human Rights in Islam (CDHR (1990), Article 18).....	76
2.7 International Standard of Privacy.....	78
2.7.1 Organisation for Economic Cooperation and Development (OECD)...	78

2.7.2 Asia-Pacific Economic Cooperation (APEC).....	83
2.8 Concluding Remarks.....	87

Chapter Three

Privacy in Islam

3.1 Introduction.....	90
3.2 The Sources of Shari’ah (Islamic Law).....	91
3.2.1 The Holy Qur’an.....	91
3.2.2 The Sunnah.....	94
3.3 Shari’ah and Some Aspects of Privacy.....	95
3.3.1 Privacy of the Home.....	95
3.3.2 Suspicion and Espionage.....	99
3.3.3 Private Correspondence.....	103
3.3.4 Confidential Conversation.....	104
3.4 The Privacy of Non-Muslim.....	107
3.5 The Privacy of the Deceased Persons.....	108
3.6 The Role of Government.....	110
3.7 Concluding Remarks.....	111

Chapter Four

Privacy and Information and Communications Technology in Jordan: *The Public Sector*

4.1 Introduction.....	114
4.2 ICT and Its social, economical and political Impacts.....	114
4.3 ICT and Its impacts on Privacy.....	117
4.4 ICT in Jordan.....	120
4.4.1 Electronic Government in Jordan.....	125
4.4.2 E-Government Initiative and Individual Privacy Concerns.....	129
4.4.2.1 Collection of Personal Information.....	135
4.4.2.2 Use and Disclosure of Personal Information.....	139
4.4.3 Privacy Impact Assessments (PIA) for the E-Government Initiative...	146
4.5 Concluding Remarks.....	149

Chapter Five

Privacy and Information and Communications Technology in Jordan: *The Private Sector*

5.1 Introduction.....	151
5.2 Economic and trade liberalisation in Jordan.....	154
5.2.1 Jordan and the World Trade Organisation (WTO).....	156
5.2.1.1 Jordan's Obligations in Telecommunications under WTO GATS.....	157
5.2.1.2 Jordan's Obligations in Banking sector under WTO GATS.....	160
5.2.2 The Jordan-US Free Trade Agreement (JUSFTA).....	164
5.2.3 The Jordan-European Association Agreement.....	173
5.2.3.1 EU-Jordan Action Plan.....	176
5.3 The Telecommunications Sector in Jordan.....	182
5.3.1 The Ministry of Information and Communications Technology (MoICT).....	186
5.3.2 Telecommunications Regulatory Commission (TRC).....	187
5.3.3 The Privacy Implications of the Telecommunications Sector in Jordan.....	191
5.3.3.1 An Online Case Study.....	192
5.4 The Banking Sector in Jordan.....	198
5.4.1 Introduction.....	198
5.4.2 The Banking System in Jordan.....	200
5.4.3 The Banking System and the ICT in Jordan.....	203
5.4.3.1 Automated Teller Machines (ATMs).....	204
5.4.3.2 Internet Banking.....	205
5.4.3.3 Telephone Banking.....	207
5.4.3.4 Credit Cards.....	208
5.4.4 The Privacy Implications of e-Banking in Jordan.....	208
5.4.5 The Extent of e-Banking Services in Jordan	210
5.4.6 The Privacy Concerns of e-Banking in Jordan.....	212
5.4.6.1 Online Privacy Consent.....	214
5.4.6.2 Transborder Data Flows (TDF).....	216
5.4.7 The Privacy Implications of Foreign Banks in Jordan: A Case Study.....	218
5.5 Concluding Remarks.....	221

Chapter Six

The Legal Landscape of Privacy Protection in Jordan

6.1 Introduction.....	225
6.2 The Legal System in Jordan.....	225
6.2.1 The Constitution of Jordan.....	226
6.2.2 The Sources of Law in Jordan.....	228
6.2.3 The Court System in Jordan.....	229
6.3 Laws Applicable to Privacy Protection in Jordan.....	235
6.3.1 Major Laws.....	236
6.3.1.1 The Jordanian Constitution and Privacy.....	236
6.3.1.2 The National Centre for Human Rights Law No 51 of 2006.....	240
6.3.1.3 The Civil Code No 43 of 1976.....	241
6.3.1.4 The Penal Code No 16 of 1960.....	244
6.3.1.5 The Law on Guaranteeing the Right of Access to Information No 47 of 2007.....	247
6.3.2 Privacy Laws Concerning Jordan’s Telecommunications Sector...	250
6.3.2.1 The Telecommunications Law No 13 of 1995.....	250
6.3.2.2 The Postal Services Law No 34 of 2007.....	254
6.3.3 Privacy Laws Concerning the Banking Sector in Jordan.....	255
6.3.3.1 The Banks Law No 28 of 2000.....	256
6.3.3.2 The Credit Information Law No 15 of 2010.....	259
6.3.3.3 The Anti-Money Laundering Laws and Regulations.....	262
6.3.3.3.1 The Anti-Money Laundering Law No 46 of 2007.....	263
6.3.3.3.2 Regulations of Anti-Money Laundering and Terrorism Financing Circular No 29 of 2006.....	265
6.4 Concluding Remarks.....	269

Chapter Seven

The Legal Landscape of Privacy Protection in the United States

7.1 Introduction.....	271
7.2 Privacy as a Constitutional Right.....	273
7.2.1 The First Amendment.....	274
7.2.2 The Fourth Amendment.....	279
7.2.3 The Ninth Amendment.....	283

7.3 US Privacy Torts Law	285
7.3.1 Intrusion upon Seclusion.....	285
7.3.2 Public Disclosure of Private Facts.....	287
7.3.3 False Light.....	290
7.3.4 Appropriation.....	289
7.4 US Federal Legislations Applicable to Privacy	294
7.4.1 Privacy Laws Concerning the Public Sector	295
7.4.1.1 Privacy Act of 1974.....	295
7.4.1.2 Freedom of Information Act (FOIA) of 1966.....	298
7.4.1.3 Electronic Freedom of Information Act Amendments (EFOIA) of 1996.....	303
7.4.1.4 Computer Matching and Privacy Protection Act of 1988.....	304
7.4.1.5 E-Government Act of 2002.....	309
7.4.2 Privacy Laws Concerning US Telecommunications Sector	312
7.4.2.1 Electronic Communication Privacy Act of 1986.....	312
7.4.2.2 Telephone Consumer Protection Act of 1991.....	316
7.4.2.3 Children’s Online Privacy Protection Act of 1998.....	320
7.4.3 Privacy Laws Concerning US Financial Sector	326
7.4.3.1 Gramm-Leach-Bliley Act (GLBA) of 1999.....	326
7.4.3.2 Fair Credit Reporting Act (FCRA) of 1970.....	331
7.4.3.3 Right to Financial Privacy Act of 1978.....	334
7.4.3.4 Bank Secrecy Act of 1970.....	338
7.5 The Federal Trade Commission (FTC)	340
7.5.1 The US Self-Regulation Approach to Privacy Protection.....	346
7.6 Concluding Remarks	350

Chapter Eight

The Legal Landscape of Privacy Protection in the European Union: *The EU Directive 95/46/EC*

8.1 Introduction	352
8.2 Background to the EU Data Protection Directive 95/46/EC	354
8.3 The Scope of the EU Data Protection Directive 95/46/EC	357
8.3.1 Article 25 and the requirement for ‘adequacy’.....	364
8.3.2 Article 26 and exemption from the ‘adequacy’ requirement.....	366
8.3.3 Article 29 and the ‘Working Party’.....	369
8.4 The US-E.U Safe Harbour Principals	375
8.4.1 Background.....	375
8.4.2 The Safe Harbour Principles.....	376
8.4.3 The Proposal for a Jordan-EU ‘Safe Harbour’ agreement.....	380
8.5 Concluding Remarks	382

Chapter Nine

Findings and a Final Thought

9.1 Introduction.....	384
9.2 Summary of Findings.....	386
9.3 Possible Policies for Privacy Protection in Jordan.....	414
9.3.1 The Self-Regulation Approach.....	414
9.3.1.1 Advantages of the Self-Regulation Approach.....	416
9.3.1.2 Disadvantages of the Self-Regulation Approach.....	418
9.3.2 The Comprehensive Approach.....	421
9.4 The Self-Regulation Approach or the Comprehensive Approach: <i>The Case of the UK Media Scandal</i>.....	429
9.4.1 Background.....	429
9.4.2 The phone Hacking and the Law.....	430
9.4.3 Analysis.....	432

A Final thought

9.5 A Model Legal Framework for Privacy Protection in Jordan.....	434
9.5.1 The Jordanian Privacy Protection Law (PPL).....	434
9.5.1.1 The Scope of the PPL.....	434
9.5.1.2 Individual Standard Notice of Information.....	437
9.5.1.3 Individual Choice and Control of Information.....	439
9.5.1.4 Limited Access.....	440
9.5.1.5 Effective Enforcement and Individual Remedies.....	440
9.5.2 The Jordanian Commission for Privacy Protection (JCPP).....	441
9.5.2.1 Regulatory Authority and Advisory Role.....	442
9.5.2.2 Independence.....	444
9.5.2.3 JCPP-Private Sector Relationship.....	445
9.5.2.4 Educational and Awareness Role.....	446

List of Figures

Figure No

1. Conceptual Framework for Privacy Protection in the Context of ICT-Jordan.....	13
2. Number of Mobile Subscribers and Penetration Rate (2005-2009).....	184
3. Number of Internet Subscribers and Penetration Rate (2005-2009).....	185
4. Number of Fixed Line Subscribers and Penetration Rate (2005-2009).....	185
5. Jordan Banking System (2009).....	203
6. The Flow of Personal Information Cycle between Jordan to the EU Member States.....	366

List of Tables

Table No

1. ICT Growth in Jordan (2003-2009).....	122
2. Telecommunications Sector Revenue in Jordan for year 2009.....	122
3. Government Agencies in Jordan connected to the e-Government Portal	144
4. Government Agencies Websites with Availability of FIPs- Jordan.....	145
5. Telecommunications Companies with Availability of FIPs-Jordan	194
6. Banks with Online Services and Privacy Policies/Statements-Jordan.....	211
7. Information Privacy Practices of Foreign Banks-Jordan.....	219

List of Appendices

Appendix A, Exhibits 1-3: Privacy Policies of Government Agencies-Jordan	479
Appendix B, Exhibits 1-9: Privacy policies/Statements of Telecommunications Companies- Jordan.....	488
Appendix C, Exhibits 1-20: Banks with Privacy Policies/Statements- Jordan.....	509
Appendix D, Directive 95/46/EC.....	544

ABBREVIATIONS

AA	Association Agreement
ACHR	American Convention on Human Rights
ALRC	Australian Law Reform Commission
AMLU	Anti-Money Laundering Unit
APEC	Asia-Pacific Economic Cooperation
CBJ	Central Bank of Jordan
CDHR	Cairo Declaration of Human Rights
COPPA	Children's Online Privacy Protection Act
DOC	Department of Commerce
DVLD	Drivers and Vehicles Licence Department
EC	European Commission
ECHR	European Convention on Human Rights
EFTA	European Free Trade Association
E-Government	Electronic Government
E-Participation	Electronic Participation
EPC	Executive Privatisation Commission
EU	European Union
FCC	Federal Communication Commission
FIPs	Fair Information Practices
FLAG	Fiberoptic Link Around the Globe
FTC	Federal Trade Commission
G2B	Government to Business
G2C	Government to Consumer
G2G	Government to Government
GATT	General Agreement on Tariffs and Trade
GOJ	Government of Jordan
EHR	Electronic Health Record
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
ID	Identification
IMF	International Monetary Fund
IT	Information Technology
JCPP	Jordanian Commission for Privacy Protection
JD	Jordan Dinar
JUSFTA	Jordan-United States Free Trade Agreement
MENA	Middle East and North Africa
MLRO	Money Laundering Reporting Officer
MoICT	Ministry of Information and Communications Technology
NCHR	National Centre for Human Rights
OECD	Organisation for Economic and Co-operation Development
OMB	Office of Management and Budget
PIA	Personal Identified Information
PPL	Privacy Protection Law

PPP	Public-Private Partnership
SAR	Suspicious Activity Report
SVC	Stored Value Card
TDF	Transborder Data Flow
TRC	Telecommunication Regulatory Commission
UDHR	Universal Declaration of Human Rights
USTDA	United States Trade and Development
WTO	World Trade Organisation

ACKNOWLEDGMENTS

In spite of much turbulence, many hurdles, obstacles and difficult times (you name it) that I faced on this PhD journey, I am so thrilled and touched to know many people who made my way towards the completion of this journey so easy, accessible, laughable and enjoyable (you name it too). This PhD thesis would not be achieved without their help, encouragement and best wishes. Their direct and/or indirect contributions should always be remembered.

For starters, I would like to thank my supervisor Dr Jakkrit Kuanpoth and co-supervisor Dr Charles Chew. I am deeply indebted to them for their unconditional support and assistance. They proved to be not just professional academics, but also great exemplars of friendship.

Also I wish to thank Dr Luke McNamara, the Dean of the Faculty of Law, for his support in difficult times. He has shown himself to be a great person who is willing to help not on academic level but on a personal level. A special thanks to Dr Warwick Gullet, the Head of Postgraduate Studies, for his support and assistance. Many thanks also go to the Faculty's staff, namely: Felicia Martin, Maria Agnew, Elizabeth Mazar, Jessica Lopez and Carla Giliberti.

I would also like to thank the following people for their help and assistance: the law librarians Elizabeth White and Lucia Tome, and the law editorial assistant Elaine Newby for her amazing work. I also thank my colleagues at the University of

Wollongong. Many thanks also to my colleagues and managers at MLC of the National Australia Bank Group, namely, Margaret Stewart, Zoe Evanegilindis, Jim Love, Belinda Burke, Claire Devenney and many more for their best wishes and support. I also, deeply thank my lovely friend Ms Najah Chami for her warmest wishes.

I also wish to thank the following persons from Jordan for their assistance: my good friend Mr Raed Almoary, a lawyer, Ms Heba Abu-Yaseen from Audi Bank-Jordan, Mr Mamon Matalqa of Telecommunications Regulatory Commission, Dr Jamal Abu Obiad and Mr Usama Alhaj of the Housing Bank for Trade & Finance.

Finally, I wish to give my heartfelt thanks to my mother who deserves gratitude beyond any limit for her prayers and blessings, Thank you mother. I would also love to thank my immediate and extended family. They wanted this to be done as much as I do. I hope that every one of them is pleased with my achievement. I would like to say to every one of them: *Thank you.*

*This work is dedicated to the memory of my beloved father-May Allah rest him
in Peace*

Mousa 1941-2008
and to my dear son, **Faris** 2007-

STATEMENT OF AUTHORSHIP

I, Akram M. Almatarneh, declare that this thesis, submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Law, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualification at any other academic institution.

Akram Almatarneh

2011

LIST OF PUBLICATIONS

Part of this thesis was originally published in:

Almatarneh, Akram, 'Privacy Implications for Information and Communications Technology (ICT): The Case of the Jordanian e-Government' (2011) 6(3) *Journal of International Commercial Law and Technology* 151-164.

Almatarneh, Akram, 'Privacy Implications for Information and Communications Technology (ICT): The Case of the Jordanian e-Government' in Sylvia M Kierkegaard (ed), *Private Law: Rights, Duties & Conflicts* (2010) 249-258.

ABSTRACT

In recent years, Jordan as a developing country has carried out extensive reforms leading to the liberalisation of its market, deregulation of some industries and privatisation of many services previously provided by the public sector. In addition, Jordan has signed multilateral and bilateral international trade agreements as major steps taken to remove trade barriers and enable the country to become an actor on the global stage. As a result of these reforms, the sector of information and communications technology (ICT) has become one of most liberalised, privatised and advanced sector in the country. It affects all aspects of the Jordanian society, including education, healthcare, employment, telecommunications, banking and commerce. However, the challenge of individual privacy protection is a particular challenge as individuals are disclosing larger amounts of personal information than ever at a time when there are no privacy protection laws. In the mean time, public and private sectors alike are using information and communication technologies to collect, use, disclose access and transfer personal information when there are no specific guidelines to regulate their practices.

This thesis examines the legal landscape of privacy protection in the context of ICT in Jordan. The thesis provides an extensive examination of privacy information practices in the public and the private sectors. It assesses and evaluates the level to which the privacy of personal information is protected and maintained by these two sectors.

For the public sector, the thesis identifies in a case study the privacy concerns of the electronic government (e-government) of Jordan. The findings of this study are surprising. Despite most government agencies in e-government portals having the ability to collect, use, disclose, and transfer personal information, only three of the forty governmental agencies have established policies with regard to privacy protection of personal information.

For the private sector, businesses from the telecommunications and the banking sectors are chosen for investigation in relation to privacy. These two industries are the largest in the country in terms of their ability to collect, use, access, and transfer personal information. The thesis develops a 'privacy questionnaire' on the personal information practices of the private sector. The "privacy questionnaire' identifies major concerns regarding individual privacy within these businesses.

The thesis discusses in detail two opposing models of the regulation of privacy. It examines the European Union approach, which is described as a rights-based approach, and the US approach, which can be regarded as non-interventionist, reliant on the market and self-regulatory mechanisms. The tensions between the two models in the EU and US culminated in the adoption of Safe Harbour Privacy Principles. The thesis examines the effects of these two models on Jordan's approach to privacy protection, given the fact that Jordan relies on both regimes for political, economical and financial support.

Finally, the thesis proposes national legislation for privacy protection. The proposed legal framework addresses, for the first time, the concept of privacy as a legal term. It also addresses privacy issues that may arise in the context of ICT in Jordan. In addition, the proposed model meets the international privacy principles and in particular, the 'adequacy' requirements stated in the EU Directive 95/46/EC.

Chapter One

General Introduction

'It is time to widen the scope of our participation in the knowledge economy from being mere isolated islands on the periphery of progress, to becoming an oasis of technology that can offer the prospect of economies of scale for those who venture to invest in our young available talent.'¹

1.1 Background to the Research

In the past few years, Jordan — as a rapidly developing country — has implemented major economic reforms in order to create an active and dynamic free economy that leads towards an information and knowledge-based society. As a strategic approach, the information and communications technology (ICT) sector has been selected by the Government of Jordan as being the single greatest driving force behind Jordan's economic success.² This sector represents a significant sector of the Jordanian economy. In 2009, the revenues of the ICT sector in Jordan were USD 2.1 billion, with IT revenues of USD 895 million and telecommunications revenues of USD 1.3 billion.³ It was estimated that the revenues derived from this sector would be USD 3 billion by 2011.⁴ Apart from the benefit to the national economy, the ICT sector in Jordan can play a beneficial role in the lives of individuals and

¹ King Abdullah II, *New Beginning Making a Difference: A view from the Developing World* (2000) Government of Jordan <www.kingabdullah.gov.jo> at 15 October 2008.

² Information Technology Association Jordan (INT@J), 'Jordan's Information Society a Fast Growing Sector for a Transforming Nation' (Economic and Social Commission for Western Asia, 2003) 1 <<http://www.mafhoum.com/press4/131jordan.pdf>>.

³ Information Technology Association-Jordan (int@j), 'ICT & ITES Industry Statistics & Yearbook' (Information Technology Association-Jordan (int@j), 2009) 10 <http://www.intaj.net/sites/default/files/2009_ICT__ITES_Industry_Statistics__Yearbook_Final.pdf>.

⁴ Ministry of Information and Communications Technology, 'National ICT Strategy of Jordan 2007-2011' (MoICT, 2007) 3 <www.moict.gov.jo> at 15 November 2008.

in the life of the society as a whole. As part of the policy promoting the ICT sector, in 2003, the Jordanian Government initiated the Electronic Government (e-Government). The e-Government initiative⁵ aims to improve the quality and efficiency of the services that the government provides to its citizens and ensure that these are provided at the lowest cost.

In the private sector, the ICT sector plays an important role in driving other major economic sectors. The information and communication technologies (ICTs), particularly the Internet, are also responsible for the growth of other sectors, including: education, employment and health care, banking, and telecommunications.⁶ For example, the number of Internet users in Jordan reached 1.127 million at the end of the year 2007,⁷ and is expected to rise to 2.78 million by year 2012.⁸ The Internet is used by individuals and businesses for different transactions (such as buying products, paying for services and paying bills online) from anywhere in the world. The latest report by the Arab Advisory Group reveals that 15.4 per cent of the Internet users in Jordan are e-commerce users. The report estimates that the number of Internet users for e-commerce purposes is around 181,000 representing 3 per cent of the total population of Jordan. The estimated spend is about USD 192 million.⁹ Furthermore, due to the low cost involved in adopting the new technology, many businesses can use it to locate consumers and find out what

⁵ Government of Jordan, *E-Government Program (2003)* Ministry of Information and Communications Technology <www.moict.gov.jo> at 15 November 2008.

⁶ INT@J, 'Jordan's Information Society', above n 2, 1.

⁷ Business Monitor International, 'Jordan Telecommunications Report Q3 2008' (Business Monitor International, 2008) 14.

⁸ Business Monitor International, 'The Jordan Lebanon & Syria Business Forecast Report Q4 2008' (Business Monitor International, 2008) 5.

⁹ Arab Advisors Group, 'Jordan Internet Users and E-Commerce survey 2010' (Arab Advisors Group, 2010) 61-71.

type of transactions they perform, The technology has provided industries with the ability to collect, access, store and transfer vast amounts of information about individuals and their transactions.

A number of steps taken by policy-makers have initiated the above developments in Jordan. To support the government's policy on ICT, the enactment and amendment of several relevant laws and regulations was required. It was necessary for the government to initiate the privatisation of some public sectors.¹⁰ In addition, Jordan's accession in 2000 to the World Trade Organisation (WTO) and its signing of multilateral and bilateral trade agreements with trade partners were significant factors leading to the rapid development of the ICT sector.¹¹

1.2 Statement of the Problem

For many people, privacy is an important concept as it relates to many other significant issues, such as: private communications and personal papers, protection of home, family, reputation, and bodily integrity. In the ICT context, and particularly for the Internet users, invasion of privacy is regarded as a major concern. For example, an American Express survey in

¹⁰ Jordan enacted the *Telecommunications Law No 13 of 1995*, amended in 2002, the *Investment Promotion Law No 16 of 1995*, the *Privatisation Law No 25 of 2000*, the *Electronic Transactions Law No 85 of 2001*, and the *Credit Information Law No 15 of 2010*.

¹¹ In 2000, Jordan became the fourth country in the world to have a free trade agreement with the United States: Ministry of Foreign Affairs, *Jordan and the Free Trade Agreement with the United States of America* <www.mfa.gov.jo> at 10 November 2008. Just two years later, on 1 May 2002, the EU Association Agreement with Jordan, namely the *Jordan-EU Euro-Mediterranean Association Agreement* (signed 24 November 1997) OJ L 129/2, entered into force (replacing the Jordan-EU Economic Cooperation Agreement of 1977) available at: <<http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/jordan/>> at 10 November 2008.

2000 of 11,000 consumers in 10 countries found that 79 per cent believed that their privacy was a significant issue.¹²

For Jordan, two recent developments have created problems in regard to individual privacy: namely the increase in the amount of information available on individuals, which has been generated by the adoption of ICTs, and the impact of privatisation on the control of the information collected.

First, the use of ICTs to communicate, collect, store and manipulate personal information has dramatically increased the level of personal information generated and exchanged, which in turn affects the individual's privacy.¹³ Concerns have been raised regarding the collection and use of information concerning individual by the government agencies. The use of new technology has increased that anxiety. One concern is that the collected information may be used for purposes other than those for which it was originally intended.¹⁴ Government agencies may misuse this personal information, for example, for retaliation against the Government's opponents, or for that matter, some personnel within government agencies'

¹² Consumers International, 'Privacy@net: An International Comparative Study of Consumer Privacy on the Internet' (Consumers International, 2001) 11. Another survey by the US National Consumer League found that privacy was one of consumers' highest concerns — 57% said that they had not bought anything online in the last 12 months because they were worried that either their credit card number or their personal information would be abused and other consumers reported that they provided false information to protect themselves: at 11 <<http://www.consumersinternational.org/media/304817/privacy@net-%20an%20international%20comparative%20study%20of%20consumer%20privacy%20on%20the%20internet.pdf>> at 8 December 2010.

¹³ William J Long and Mark Pang Quek, 'Personal Data Privacy Protection in an Age of Globalisation: the US-EU Safe Harbour Compromise' (2002) 9(3) *Journal of European Public Policy* 325, 329.

¹⁴ Jonathan P Graham, 'Privacy, Computers and the Commercial Dissemination of Personal Information' (1986) 65 *Texas Law Review* 1395, 1402.

may, for their own purposes, misuse personal information to which they have access.

Under a controversial Regulation, *'Instructions for Regulating the Work of the Internet Centres and Cafes and the Bases for their Licensing'*¹⁵ issued in 2001 by the Ministry of Interior, Internet centre and cafés must collect all 'personal data on [a] special registration form', with such information including the 'user's names, national identity numbers, the time of use'.¹⁶ They are also required to collect the 'fixed IP address of the Internet access point and monthly log files showing which sites had been visited and by whom'.¹⁷ While the Regulation requires the Internet centres and café operators to 'maintain the confidentiality of all data',¹⁸ it authorises operators to pass on the confidential data to government agencies in accordance with terms and conditions as required by the law.¹⁹

The Government justifies this Regulation on the basis of national security. It may help to track down some individuals who may pose threats to the country. It may also prevent some illegal activities such as: transmission of pornographic images or selling illicit products.

¹⁵ Ministry of Interior, *Instructions for Regulating the Work of the Internet Centres and Cafes and the Bases for their Licensing* (2001) Ministry of Interior <http://www.reach.com.jo/Downloads/Legislative/Internet_Cafes_Regulations.pdf> at 3 December 2010.

¹⁶ Ibid art 6(1).

¹⁷ Ibid art 6(2).

¹⁸ Ibid art 6(3).

¹⁹ Ibid art 11(2).

The author, however, believes that this Regulation is unconstitutional as it invades personal freedom.²⁰ Such a regulation grants the Government the ability to control information that individuals try to access or acquire. It is also unfair for Internet users to disclose their personal information to operators who are a third party. A genuine privacy concern is that operators can disclose and transmit personal information about the users without their consent.

Further, this Regulation contradicts the Statement of Government Policy 2007 on the Information and Communication Technology and Postal Sectors.²¹ According to this policy, the Government requires that open market principles apply to the IT sector; therefore, it could be surmised that the Government requires that no restrictive regulations be applied to the ICT sector.

Furthermore, the introduction of surveillance technology without a legal framework for the use of the technology leaves the door wide open for privacy invasion. In 2006, a state-owned company in Jordan developed an electronic warfare system that has the ability to intercept and analyse all types' of communications in the country.²² An Electronic Warfare Unit within the Jordanian Military is responsible for randomly intercepting telephone calls made by ordinary citizens and analysing their conversations.

²⁰ Article 7 of the Jordanian Constitution states that 'Personal Freedom shall be guaranteed.'

²¹ Government of Jordan, 'Statement of Government Policy 2007 on the Information & Communications Technology & Postal Sectors' (Ministry of Information and Communications Technology, 2007) 25, para 86 <www.moict.gov.jo> at 20 November 2008.

²² Middle East Newslines, *Jordan Develops EW Suite* (2008) Middle East Newslines <www.menewslines.com> at 8 December 2010.

There are many questions relating to the use of data surveillance technology: such as, ‘Will data surveillance be used in court as evidence for purposes other than traffic control and criminal activities?’; ‘Will data surveillance be used by third parties?’; and ‘What guarantees are provided to individuals where there are errors in regard to this data?’.

Second, the privatisation of many formerly public enterprises or operations in the trade and finance sectors has made it difficult for Jordan to monitor and regulate multinational corporations involved in the transfer of personal information out of the country.²³ In spite of the benefits brought by the privatisation process to the Jordanian economy, threats to individuals’ privacy in the private sector can also be identified. Foreign banking and telecommunication businesses operating in Jordan may use ICTs to collect, store, access and process individuals’ personal information. These businesses can transfer this information to branches or offices outside Jordan. To date there has been no law preventing or regulating such transfer. For example, if the telecommunications company ABC based in country A would like to open another branch in Country B, the new branch could collect, store and transfer all data of its clients from B to A. The company ABC based in A could then sell this data to a third party, in this example perhaps an insurance firm based in country D. If the supposed country B is Jordan, under the current laws of Jordan, there is no existing legal framework that could prevent these practices (transfer and/or sale of personal information) occurring. This hypothetical example becomes more complicated if these countries have

²³ Long and Quek, above n 13, 329.

different laws and regulations for privacy protection. If this were so, the level of privacy protection for the information changes as its location changes from country to country. The responsibilities of individuals and multinational businesses also alter.²⁴ This means that clients or customers in country A and/or D would have legal remedies if their privacy were being violated, as these countries have privacy protection laws. In contrast, clients or customers in Jordan may not have a legal basis for compensation when their privacy is violated by company ABC. This scenario applies to other type of businesses, such as the banking industry.

1.3 Research Questions

The development of the ICT sector in Jordan is seen as a success story for one of the developing countries. Despite the success, a huge gap in regards to individual privacy protection exists. It is unquestionable that privacy protection laws in Jordan are insufficient and inadequate. This due to the fact that privacy — as a legal concept — has not yet evolved in Jordan. The term ‘privacy’ in Jordan has always been related to either family and/or women. Therefore the main responsibility of this research is to examine the insufficiency and the inadequacy of the Jordanian law with respect to privacy. In addition, the research examines the following questions in order to propose a desirable approach to privacy protection.

The first question to be examined is:

²⁴ Priscilla M Regan, 'The Globalization of Privacy: Implications of Recent Changes in Europe' (1993) 52(3) *American Journal of Economics and Sociology* 257, 259.

1. 'Do individuals in Jordan have the right to privacy?' and associated with this question is whether this right guaranteed by the Constitution, International Treaties and/or by traditions and beliefs?
2. 'Do individuals in Jordan need specific legislation to protect their privacy in the ICT sector or, can Jordan rely only on market mechanisms such as self-regulation, technology or government guidelines for protecting privacy?'
3. 'Is self-regulation the most appropriate approach for Jordan?'
4. 'What alternatives may be suitable for the Jordanian legal system to protect privacy?'
5. The main question, however, and one that constitutes the conceptual framework for this research is: 'What is the best approach to privacy protection within the Jordanian context?'

1.4 Conceptual Framework

There are two main approaches for developing a conceptual framework for privacy protection. The first approach is to see privacy as a property right while the second approach views privacy as part of human rights.

According to the former, personal information or the content of personal communications is seen as the property of the person in question. Therefore, the person who conveys the information would have a legal right to control the use of that information and could take legal action against those who misuse the information.²⁵ In this regard, Alan Westin suggests that 'personal

²⁵ Priscilla M Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (1995) 34.

information thought of as the right of decision over one's private personality, should be defined as a property right.²⁶ In *Olmstead v United States*,²⁷ the majority of the Supreme Court applied this approach of privacy interests when it upheld Olmstead's conviction and rejected his constitutional challenges in regards to the Fourth Amendment.²⁸

The above decision, however, was overruled when the Court in *Katz v United States*²⁹ decided that the subject of protection under the Fourth Amendment was people, not places. As a result, there is no need for physical trespass or seizure of tangible material. But the Court warned in this case that 'the Fourth Amendment could not be translated into a general "right to privacy"' and recognised that virtually every governmental action interfered with personal privacy to some degree.³⁰ It only gave indications of the limits of governmental powers to 'invade' that privacy in particular, and noted that other aspects of privacy may be covered by other Amendments.³¹

²⁶ Alan F Westin, *Privacy and Freedom* (1967) 324.

²⁷ *Olmstead v United States*, 277 US 438 (1928).

²⁸ The Fourth Amendment of the *US Constitution* states: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' Text available at the National Archives of the Government of the United States of America: *The Bill of Rights* (comprising Amendments 1–10 of the *Constitution of the United States of America*) <http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html>; see also the *Constitution of the United States of America*, National Archives of the Government of the United States of America <http://www.archives.gov/exhibits/charters/constitution_transcript.html> at 26 November 2010.

²⁹ *Katz v United States*, 389 US 347 (1967).

³⁰ *Katz v United States*, 389 US 347 (1967), n 5. See also Regan, *Legislating Privacy*, above n 25, 36.

³¹ The First Amendment, for example, imposes limitations upon governmental abridgment of 'freedom to associate and privacy in one's associations'. *NAACP v Alabama*, 357 US 449, 462 (1958). The Third Amendment's prohibition against the unconsented peace-time quartering of soldiers protects another aspect of privacy from governmental intrusion. To some extent, the Fifth Amendment too 'reflects the Constitution's concern for ... the right of each individual "to a private enclave where he may lead a private life"'." *Tehan v Shott*, 382 US 406, 416 (1966). Virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that interference violates a command of the United States Constitution.

The second approach views privacy as a set of values that are well connected to the natural persons. Because privacy can be supportive of human values such as: honour, freedom, autonomy and reputation,³² it is imperative to categorise it as a human right. A good example of a legal system treating privacy as a human right is that of the European Union (EU). The European Union deemed the best approach to protecting this right was through the adoption of a comprehensive approach. Thus the European Union introduced the *European Union Directive on the Protection of Personal Data (EU Directive 95/46/EC)*, which expressly states that the right to privacy is a fundamental right and freedom of natural persons. A general argument underlying the Directive is that treating personal information as property would have the undesirable consequence of placing responsibility on individuals to protect their own interests. Without an external authority imposing and enforcing regulations on business organisations in both private and public sectors, individual privacy is most likely to be violated.³³

The figure below shows how the Jordanian legal system can be influenced by these two approaches. This is due to trade and governmental interactions with both the United States and the EU. In the absence of any clear specific legislation to protect privacy, the ICT industry has been influenced by both these approaches. The United States apparently has a significant influence on

³² 'Honour' and 'reputation' are two different concepts, at least from the author's perspective. A person has only one honour and many different types of reputation, such as: financial reputation, health reputation and academic reputation, etc; while honour is mainly connected to either someone's family or women. For example, a woman's reputation will be damaged if a criminal sexually assaulted her, while her honour will be shattered if she has committed adultery. Her reputation as a healthy single woman or as a healthy virgin who is available for marriage may be damaged.

³³ Detlev Zwick and Nikhilesh Dholakia, 'Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right' (2001) 11(2) *Electronic Markets* 116, 119.

Jordan's policy on privacy protection for a number of reasons. First, as a result of the *Jordan-US Free Trade Agreement* (JUSFTA),³⁴ the United States is considered the main exporter of new technology to Jordan. For Jordan, JUSFTA is seen as a successful step in achieving economic growth in the ICT sector. It eliminates duties and commercial barriers to bilateral trade in goods and services originating in the United States and Jordan. This agreement presents Jordanian IT companies with a wealth of business opportunities with their US based counterparts.³⁵

Second, the United States champions 'free flow' and regards data protection laws as erecting non-tariff trade barriers that protect national industries and communications providers.³⁶ With respect to privacy, the United States-Jordan Joint Statement on Electronic Commerce recognises that:³⁷

ensuring the effective protection of privacy with regard to the processing of personal data on global information network is necessary as is the need to continue the free flow of information.

It appears to say that the right of privacy is balanced against the free flow of information. Therefore, the motivation to ensure privacy protection in US-Jordan agreements is fundamentally based on economic benefits rather than the value of privacy as a human right. A hypothetical question that could be asked is whether a renewed JUSFTA could be signed if Jordan refused to

³⁴ *Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Agreement (Jordan-US Free Trade Agreement (JUSFTA)* signed 24 October 1999 (entered into force 17 December 2001).

³⁵ INT@J, 'Jordan's Information Society', above n 2, 17.

³⁶ Regan, 'Globalisation of Privacy', above n 24, 260.

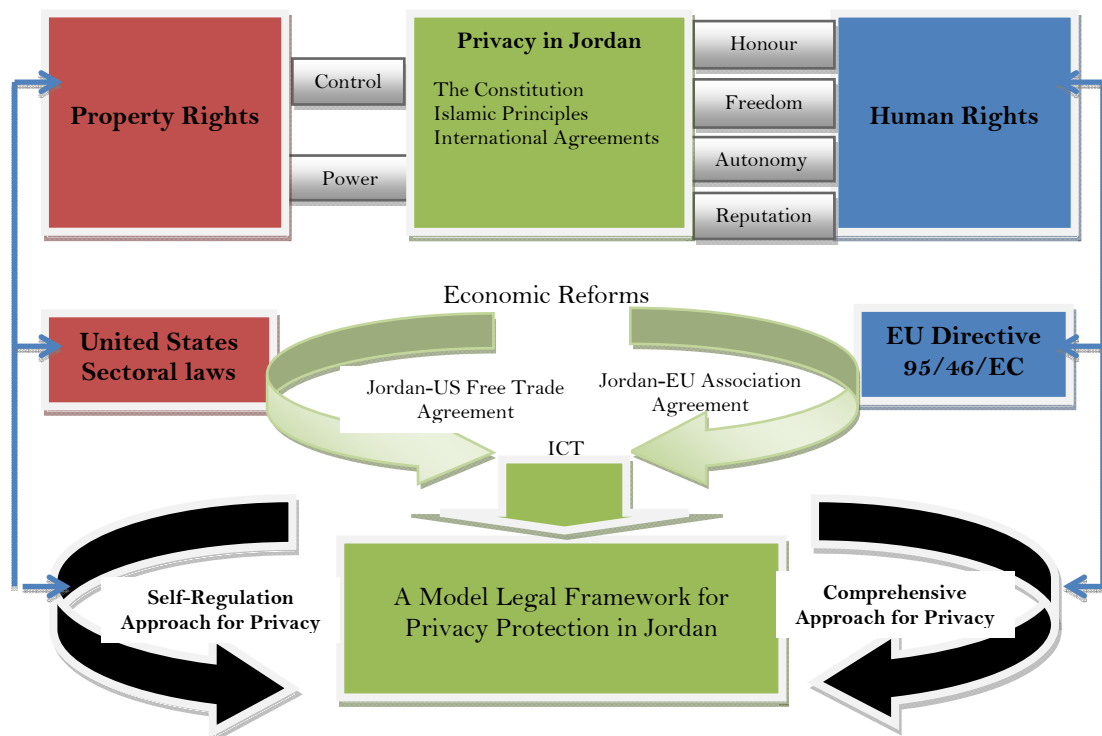
³⁷ Text of the *US-Jordan Joint Statement on Electronic Commerce* (undated) <www.jordanusfta.com/documnets/joint_statement_on_e-commerce.pdf> at 10 November 2008.

agree to the free flow of information clauses on the grounds that they might violate Jordanians' personal privacy?

Finally, Jordan has been the primary recipient of foreign assistance from the United States. For over fifty years, the United States has built schools, roads and waterways and has assisted in fighting unemployment and disease. In the year 2003, the United States provided Jordan with USD 950 million in foreign economic assistance. As a result, Jordan has become one of the largest of US aid recipients.³⁸ This means that Jordan could be under political and economical pressure from the United States to adopt certain policies and reforms.

Figure 1

A Conceptual Framework for Privacy Protection in the ICT-Jordan



³⁸ United States Agency for International Development, 'USAID/Jordan Strategy 2004-2009: Gateway to the Future' (US Agency for International Development, 2003) 6 <http://pdf.dec.org/pdf_docs/PDABZ632.pdf> at 20 November 2008. A further supplemental appropriation of USD 700 million was approved for the following year, 41.

The above figure shows that a second approach that could have an even greater impact on Jordan's policy towards privacy protection is the European Union (EU) approach. On 24 November 1997, Jordan signed an Association Agreement with the EU which entered into force on 1 May 2002, replacing the *Jordan-EU Cooperation Agreement of 1977*.³⁹ The Association Agreement provides a comprehensive framework for the economic, political and social dimensions of the EU-Jordan bilateral relations. Its main aim is to create a free trade area between Jordan and the EU over a period of 12 years, and help increase economic growth for the business community.⁴⁰ Additionally, and most importantly, the concept of privacy is considered to be a fundamental human right in the EU. The adoption of the *EU Directive 95/46/EC* was a result of the interpretation of 'the right to respect for his private and family life, his home and his correspondence' as enshrined in Article 8 of the *European Convention on Human Rights (ECHR)*.⁴¹ The concept of privacy as a fundamental human right is also common to some cultures which are founded on Islamic values and principles; however, although Islam strongly protects individual privacy, laws in Jordan are insufficient to maintain this right.

³⁹ *Jordan-EU Euro-Mediterranean Association Agreement* (signed 24 November 1997) OJ L 129/2 [2002] (entered into force 1 May 2002) <http://www.agreements.jedco.gov.jo/main/eu_doc/eu_agreement.html> at 15 November 2008.

⁴⁰ Foreign Ministry of Jordan, *Jordan and the European Union* (2008) Jordan Foreign Ministry <www.mfa.gov.jo> at 13 November 2008.

⁴¹ *Convention for the Protection of Human Rights and Fundamental Freedoms* ('*European Convention on Human Rights*' ('ECHR')), opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 8(1). Article 8(2) moreover states that 'there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

In summary and in terms of trade, the most recently available figures (June 2011) reveal that trade with both the 27 member EU (EU27) and the United States is substantial with the US the nation's major export destination (the EU27 ranks seventh) while the EU27 is the major source of imports (with the US ranking fourth), with the EU27 ranked second only to Saudi Arabia in terms of total trade (and the US fourth).⁴² Such a substantial level of trade also places a degree of pressure on a country to ensure neither the EU27 nor the US is advantaged in any privacy protection measures.

This research favours the second approach to privacy as a basis for possible reform in Jordan — that is, privacy must be explicitly stated as a fundamental human right. The legal protection currently provided to individual privacy in the context of the exponential growth in the use and sophistication of ICT is insufficient and inadequate. Although the *Jordanian Constitution*, the international treaties to which Jordan is signatory, and Islamic law (*Shari'ah*) consider privacy as a fundamental human right, the protection of privacy in Jordan, however, remains insufficient. For example, on one hand, the *Jordanian Constitution* specifically recognises a limited right

⁴² DG Trade Statistics, *Jordan: EU Bilateral Trade and Trade with the World* (DG Trade, 8 June 2011), http://trader.ec.europa.eu/doclob/docs/2006/September/tradoc_113404.pdf. Note: the respective figures are Imports (expressed as a percentage of total imports) EU27 21% (2,388 million euros); USA 6% (693 million euro); Exports USA 16% 689 million euros; EU27 4% 164 million euros. Total value of trade (expressed as a percentage of total trade with major trading partners and including both imports and exports records EU27 at 16% (2,552 million euros), US 9% (1,381 million euros). (Note all percentages rounded to nearest whole per cent; all figures to nearest million euro).

to privacy, but these rights are regularly circumscribed by the law in practice.⁴³ Article 10 of the Constitution stipulates:

Dwelling houses shall be inviolable and shall not be entered except in the circumstances and the manner prescribed by law.⁴⁴

The above Article can be directly traced to some verses of the *Holy Qu'ran*, the main source for Islamic law (*Shari'ah*). These verses provide a clear message of respect for the privacy of the home:

O ye who believe! Enter not houses other than your own, until ye have asked permission and saluted those in them: that is best for you, in order that ye may heed (what is seemly).⁴⁵

If ye find no one in the house, enter not until permission is given to you: if ye are asked to go back, go back: that makes for greater purity for yourselves: and Allah knows well all that ye do.⁴⁶

With respect to communications, Article 18 of the *Jordanian Constitution* stipulates:

All postal, telegraphic and telephonic communications shall be treated as secret and as such shall not be subject to censorship or suspension except in circumstances prescribed by law.⁴⁷

In practice, however, by introducing the Regulations on the Internet Cafes, the government has violated these constitutional restrictions.

⁴³ Privacy International, *Privacy and Human Rights: Constitutional Privacy Framework* (2007) Privacy International <<http://www.privacyinternational.org>> at 21 November 2008.

⁴⁴ *Constitution of the Hashemite Kingdom of Jordan*, adopted 1 January 1952, <http://www.kinghussein.gov.jo/constitution_jo.html> at 1 July 2008 (*Constitution of the Hashemite Kingdom of Jordan* 1952).

⁴⁵ *Surat No 24 – An-Nur, Section 4, Aya 27, Holy Qur'an*, 1011. Note, unless otherwise stated, all quotations from the *Holy Qur'an* are from: *The NOBLE QUR'AN: Translation of the Meanings of the Noble Qur'an in the English Language*: by Dr Muhammad Taqi-ud-Din al-Hilali and Dr Muhammad Muhsin Khan (King Fahd Complex for the Printing of the HOLY QUR'AN).

⁴⁶ *Surat No 24 – An-Nur, Section 4, Aya 28, Holy Qur'an*, 1011.

⁴⁷ *Constitution of the Hashemite Kingdom of Jordan* 1952, art 18.

On the other hand, the adoption of a self-regulatory approach in ICT is believed to be inadequate. Although its proponents claim that the self-regulatory approach provides efficiency, flexibility, increased incentives for compliance and reduced costs,⁴⁸ its biggest disadvantages remain the lack of enforcement mechanisms and the scarcity of legal options for individuals adversely affected.⁴⁹ In the case of Jordan, the Telecommunications Regulatory Commission (TRC) which is responsible for implementing the government policy on ICT has no specific mechanisms to allow individuals to address their privacy concerns.⁵⁰

1.5 Aims and Objectives of the Research

The thesis mainly aims to propose a model legal framework for privacy protection in the context of ICT in Jordan. In order to achieve this aim, an exploration is required of the current practices in the public and private sectors in regard to individual privacy. In this regard, the thesis examines privacy policies and guidelines, and determines whether these policies and guidelines provide adequate and sufficient privacy protection.

The thesis seeks to achieve the following objectives:

a) *Define the concept of privacy.* In an attempt to develop a working definition of 'privacy', the following chapter (Chapter Two) discusses the meaning of 'privacy' and examines how different concepts of privacy result in different

⁴⁸ Angela J Campbell, 'Self-Regulation and the Media' (1999) 51 *Federal Common Law Journal* 715–17.

⁴⁹ Joann M Wakana, 'The Future of Online Privacy: A Proposal for International Legislation' (2003) 26 *Loyola of Los Angeles International and Comparative Law Review* 151, 160.

⁵⁰ The Jordanian Telecommunications Law has given the TRC many tasks, none of which address privacy concerns. See Article 5, Chapter III, of *Telecommunications Law No 13 of 1995* as amended by Law No 8 of 2002.

regulations. It also reviews the importance of privacy, which has been expressed in several international instruments to which Jordan is a signatory.

b) *Examine the historical principles of privacy in Islam and link them to the modern definitions of privacy.* Chapter Three provides some examples where the *Shari'ah* (Islamic law) protects individual privacy. This linkage assists to further develop a working definition of 'privacy' as the *Shari'ah* is a major source of legislation for Jordanian law.

c) *Investigate the public sector's position regarding individual privacy protection.* It is important to assess the extent to which individual privacy is protected and maintained within and by governmental agencies. The assessment (presented in Chapter Four) is necessary for an appropriate and suitable proposal to address privacy concerns in the public sector.

d) *Identify privacy concerns and threats to individual in the private sector.* The intention of this objective is to measure the extent to which current practices by the private sector violate individual privacy. This is undertaken in Chapter Five.

e) *Critically review and analyse the current laws that maybe applicable to privacy in Jordan.* At the time of writing, Jordan has no specific privacy laws or regulations to address individual concerns; however Chapter Six will examine Jordan's current legal landscape.

f) *Evaluate the appropriateness of US and EU privacy approaches for use in Jordan.* This objective is important as these approaches have opposing models of privacy regulation and both the US and the EU and their models may have an influence on Jordan in its selection of a model for implementation.

Therefore, it is necessary that each approach be examined in detail; hence this is undertaken in separate chapters (the US in Chapter Seven, and the EU in Chapter Eight).

g) *Explore opportunities for privacy reforms in Jordan.* This is an ambitious objective that is addressed in Chapter Nine. For the first time, this thesis proposes privacy legislation with specific details to regulate privacy issues.

1.6 Approach and Methodology

The thesis presents a critique of the current legal landscape as well as actual practices in regards to privacy protection in Jordan. It aims to examine whether or not the Jordanian legal system adequately and sufficiently addresses the issue of individual privacy in the light of recent economic reforms and rapid technological advancements in the ICT sector.

The thesis adopted an empirical methodology to investigate the current privacy rules and information practices in Jordan in two sectors. First, for the public sector, an online-based survey was conducted of a number of governmental agencies that have an online presence on the World Wide Web (websites). This survey was completed between 4 June 2009 and 25 June 2009 and the number of government agencies investigated was 40.

Second, for the investigation in the private sector, two specific areas of business were selected for an online-based study: the banking and the telecommunications industry. The intention of this study's use of a survey of private business entities was to obtain a description of a business's practices

regarding personal privacy, one which would enable the author to assess whether the private sector provides sufficient privacy protection. The private sector study covered 15 local banks, 8 foreign banks and 4 major telecommunications companies in Jordan. The online-based study was conducted between 12 October 2010 and 2 January 2011.

The above methods were aimed at gaining information regarding the following issues:

- a) The number of governmental agencies and private companies that provide policies and guidelines on their privacy practices;
- b) The effectiveness of privacy policies and guidelines in protecting individual privacy;
- b) The contents of privacy policies and guidelines;
- c) The compatibility of these privacy policies with international privacy standards; and
- d) The enforceability of privacy policies and guidelines in Jordan.

Furthermore, the thesis provides a comparative study of two opposing models of privacy regulation. It explains in detail the European Union approach, which is described as a 'rights-based' regime, and the US approach, which embodies the adoption of self-regulatory mechanisms for privacy protection. These two approaches were chosen for this comparative study as both regimes have a long history of addressing privacy concerns and associated issues in general and in the context of ICTs in particular, and both sources (the European Union and the United States) are influential in the

Jordanian context. Further, as mentioned above, both regimes have different understandings of the concept of privacy. The European Union has adopted comprehensive regulation through the *EU Directive 95/46/EC*, while the United States rejects all attempts to provide comprehensive legislation for privacy. Instead, the United States has favoured a piecemeal approach by enacting legislation to regulate certain businesses when it has been revealed that particular unlawful practices and activities have occurred (for example, the use private information for defamatory purposes).

The thesis relies on a legal survey of countries and will involve the collection of relevant laws and regulations. These will largely be obtained online where available from websites, but also by contacting agencies directly to obtain the latest laws, regulations and briefs.

There are several procedures to support the above. These procedures are:

1. Examination to primary materials. Materials include, but are not limited to, statues and regulations such as:
 - *Telecommunications Law No 13 of 1995* (amended by *law No 8 of 2002*), *Electronic Transaction Law No 85 of 2001*, the *Law of Credit Information No 15 of 2010*, and the *Regulation of Anti-Money Laundering and Terrorism Financing*, Circular No 29/2006,
 - *EU Directive 95/46/EC*,
 - Safe Harbour Principles,
 - Court decisions in the United States, the European Union and Jordan.

2. Collection and review of secondary sources relevant to the research topic. Secondary sources include: books, journal articles, electronic sources and government publications.
3. Review of the privacy policies of the private sector, by studying selected companies in the field of information and communication technology. Telecommunications and banking are the main two areas in the private sector to be investigated. The purpose of the study is to learn about business practices in these areas in regard to extent that they offer privacy protection.

1.7 Literature Review

Legal and philosophical interest in the right to privacy has intensified in recent years in tandem with the rapid development of new technologies.⁵¹ As this thesis seeks to provide a legal framework for privacy protection in the context of ICT in Jordan, it must review some of the most distinguished definitions of the concept of privacy as it has been argued that one of the main problems in implementing a law of privacy is the failure to provide an accepted working definition of privacy.⁵²

Currently, there is no consensus in the legal and philosophical literature on a definition of privacy.⁵³ Privacy is a term used with many meanings.⁵⁴ For Hyman Gross, privacy is 'the condition of human life in which acquaintance

⁵¹ Barbara von Tigerstrom, 'Protection of Health Information Privacy: The Challenges and Possibilities of Technology' (1998) 4 *Review of Current Law and Law Reform* 44.

⁵² Dudley J Moore, *Privacy: The Press and the Law* (2003) 10.

⁵³ Richard B Parker, 'A Definition of Privacy' (1974) 27(2) *Rutgers Law Review* 275.

⁵⁴ Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89(3) *The Yale Law Journal* 421, 424.

with a person or with affairs of his life which are personal to him is limited'.⁵⁵ Charles Fried considered privacy as a form of power; he defined it as 'the control over knowledge about oneself'.⁵⁶ On this basis then, 'the only way to give a person this control is to give him a legal title to control'.⁵⁷ One of the most distinguished definitions of privacy is that provided by Alan Westin who defines privacy as 'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.⁵⁸ However, one definition of privacy that has attracted academic and public attention alike is 'the right to be let alone'.⁵⁹ This definition (attributed to Thomas Cooley) was popularised by Samuel Warren and Louis Brandeis in 1890 when they referred to that definition in their article, 'The Right to Privacy'.⁶⁰ They also argued that: it was

necessary for the legal system to recognize the right to privacy because when information about an individual's private life is made available to others, it tends to influence and even to injure the very core of an individual's personality — his "estimate of himself".⁶¹

The above definitions, however, were criticised by some legal experts on the issue of privacy. Daniel Solove argued that considering privacy as a 'control-

⁵⁵ Hyman Gross, 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34, 35.

⁵⁶ Charles Fried, 'Privacy' (1968) 77 *The Yale Law Journal* 475, 483.

⁵⁷ *Ibid* 493.

⁵⁸ Westin, above n 26, 7.

⁵⁹ Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

⁶⁰ As noted by Dorothy J Glancy, 'The Invention of the Privacy' (1979) 21(1) *Arizona Law Review* 1, 3 [n 13], where she refers to Warren and Brandeis attributing its use to Cooley in his *Treatise on the Law of Torts* (1879).

⁶¹ Glancy, above n 60, 2.

over-information' can be viewed as 'too narrow a conception'.⁶² According to Solove, this definition 'excludes those aspects of privacy that are not informational; such as the right to make certain fundamental decisions about one's body, reproduction, or rearing of one's children'.⁶³ Solove, in his distinguished article 'Conceptualising Privacy', proposed a new approach to privacy. This approach is based on 'understanding privacy rather than a definition or formula for privacy'.⁶⁴ Indeed, it

provides guidance in identifying, analyzing and ascribing value to a set of related dimensions of practices in order to aid in solving problems, assessing costs and benefits and structuring social relationships.⁶⁵

The above definitions of privacy may cover most aspects of privacy, the primary focus of this research, however, is on 'information privacy' in the context of ICT. Arthur Miller has defined privacy in this context as 'the individual's ability to control the circulation of information relating to him'.⁶⁶ In other words, privacy is 'the right to control when, how and by whom personal information about oneself is communicated to and used by others'.⁶⁷ Personal information, in turn, is defined by the Australian Law Reform Commission (ALRC) as 'information or an opinion, whether true or not, and

⁶² Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1110.

⁶³ *Ibid.*

⁶⁴ *Ibid* 1129.

⁶⁵ *Ibid.*

⁶⁶ Arthur Raphael Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (1971) 40.

⁶⁷ Sandra Byrd Petersen, 'Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?' (1995) 48 *Federal Communications Law Journal* 163, 164.

whether recorded in a material form or not, about an identified or reasonably identified individual'.⁶⁸

Although there are different opinions on the definition of privacy, much of the scholarly literature, however, agrees to a great extent that privacy is important. In his remarkable book, *Privacy and Freedom*, Alan Westin, examined the significance of privacy for individuals and groups in democratic states. According to Westin, the following functions can be provided by privacy to those individuals and groups. First, it provides 'personal autonomy; privacy satisfies the human desire to avoid being manipulated or dominated by others'.⁶⁹ Second, it provides opportunity for emotional release. Here privacy performs a protective function by providing moments of less intense stress amongst the periods of anxiety and uncertainty which are part of daily life, and allowing persons to 'lay aside their masks for rest'.⁷⁰ Third, it provides the opportunity for self-evaluation. '[E]very individual needs to integrate his/her experiences into a meaningful pattern and to exert his/her individuality on events', and for this process of self-evaluation, says Weston, 'privacy is essential'.⁷¹ Finally, privacy provides opportunity for sharing confidences and intimacies.⁷²

Furthermore, Ruth Gavison claimed that privacy is essential to democratic government because it fosters and encourages the moral autonomy of

⁶⁸ Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108, (2008) 309.

⁶⁹ Westin, above n 26, 33.

⁷⁰ Ibid 35-6.

⁷¹ Ibid 36.

⁷² Ibid 38.

citizens, a central requirement for a democracy. Gavison continues that a country might restrict certain activities, but it must allow some liberty of political action if it is to remain a democracy.⁷³ Gavison states

This liberty requires privacy, for individuals must have the right to keep private their votes, their political discussions and their associations if they are to be able to exercise their liberty to the fullest extent. Privacy is crucial to democracy in providing the opportunity for parties to work out their political positions, and to compromise with opposing factions, before subjecting their positions to public scrutiny. Denying the privacy necessary for these interactions would undermine the democratic process.⁷⁴

The above statement indeed provides a great explanation for the current situation in Jordan. One of the reasons behind the slow progress in democracy is that individuals do not enjoy much autonomy. 'Autonomy' refers to 'the underlying capacity of individuals to form and act on their notions of the good when deciding how to live their lives'.⁷⁵ Government agencies have always played a role that extended to being able to interfere in an individual's life. Interference with the right to vote⁷⁶ and with the formation of political associations (despite a degree of freedom enshrined in the Constitution),⁷⁷ for example, restricts individual choice, blocks channels

⁷³ Gavison, above n 54, 456.

⁷⁴ Ibid.

⁷⁵ Paul M Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1994) 80 *Iowa Law Review* 553, 560.

⁷⁶ Despite Article 67(iii) of the *Constitution of the Hashemite Kingdom of Jordan* which indicates the punishment of those who 'adversely affect the will of voters'.

⁷⁷ There is a degree of freedom of association and for the formation of political parties permitted: See *Constitution of the Hashemite Kingdom of Jordan* art 16:

(i) Jordanians shall have the right to hold meetings within the limits of the law.

(ii) Jordanians are entitled to establish societies and political parties provided that the objects of such societies and parties are legitimate, their methods are peaceful, and their by-laws are not inconsistent with the provisions of this Constitution.

(iii) The establishment of societies and political parties and control of their resources shall be regulated by law.'

of political change and, eventually, dooms democracy.⁷⁸ In Jordan, individuals who seek government employment, for example, will avoid expressing their political views, despite Constitutional guarantees for some freedom of expression,⁷⁹ for fear that they will not be employed. Indeed, most employment decisions are based on grounds that have nothing to do with genuine occupational qualifications. In a recent poll conducted by the Centre for Strategic Studies at the University of Jordan, 18.9 per cent of respondents believed that ‘the spread of financial and administrative corruption, favoritism and nepotism’ is the most prominent obstacles to democracy in Jordan.⁸⁰ In addition, 78 per cent of the respondents in this poll stated that they cannot publicly criticise or disagree with the government without exposing themselves and their family members to persecution related to their security or livelihoods.⁸¹

The primary point to be gained from the above literature is that privacy has been widely recognised as an important value for both individuals and society. This recognition does not, however, translate into success in converting the value into a clearly defined, protectable legal standard.⁸² Ruth

⁷⁸ Schwartz, above n 75, 561.

⁷⁹ See *Constitution of the Hashemite Kingdom of Jordan* art 15, which clearly states that:

‘(i) The State shall guarantee freedom of opinion. Every Jordanian shall be free to express his opinion by words of mouth, in writing, or by means of photographic representation and other forms of expression, within the limits of the law.

(ii) Freedom of the press and publications shall be ensured within the limits of the law.

(iii) Newspapers shall not be suspended from publication nor their permits be withdrawn except in accordance with the provisions of the law.

(iv) In the event of the declaration of martial law or a state of emergency, a limited censorship on newspapers, pamphlets, books and broadcasts in matters affecting public safety or national defence may be imposed by law.

(v) Control of the resources of newspapers shall be regulated by law.’

⁸⁰ Faris Braizat, ‘Democracy in Jordan 2007’ (Centre for Strategic Studies-University of Jordan, 2007) 11, avail <www.css-jordan.org> at 22 April 2009.

⁸¹ *Ibid* 10.

⁸² Regan, *Legislating Privacy*, above n 25, 41.

Gavison suggests that, for privacy to be recognised by any legal system, privacy must be ‘distinct and coherent’.⁸³ Privacy, as suggested by Gavison, must have coherence in three contexts. First, privacy must be ‘a neutral concept [enabling people] to identify when a loss of privacy has occurred so that discussions of privacy and claims to privacy can be intelligible’.⁸⁴ Second, ‘privacy must have coherence as a value’, as claims for its protection are ‘compelling only if losses of privacy are sometimes undesirable and if those losses are undesirable for similar reasons’.⁸⁵ Third, privacy must be a concept that enables individuals to identify those occasions calling for legal protection, because the law ‘does not interfere to protect against every undesirable event’.⁸⁶

The legal recognition of a right to privacy has been expressed in many international and national documents. Internationally, Article 12 of the *Universal Declaration of Human Rights* (UDHR 1948) deals expressly with privacy. It provides:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.⁸⁷

While itself non-binding, the UDHR has served as a guide and a ‘stepping stone’ to binding instruments, including the *International Covenant on Civil*

⁸³ Gavison, above n 54, 422.

⁸⁴ *Ibid* 423.

⁸⁵ *Ibid*.

⁸⁶ *Ibid*.

⁸⁷ Article 12 of the *Universal Declaration of Human Rights*, GA Res 217A (iii), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948). Text avail <<http://www.udhr.org/UDHR/>> at 6 November 2008.

and Political Rights (ICCPR) and the *International Covenant on Economic, Social and Cultural Rights* (ICESCR). Article 17 of the ICCPR expressed privacy as a human right in Article 17. This states that:

1. No one shall be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.⁸⁸

Privacy as a human right is also well established in the European Union (EU) where the provisions of the *European Convention on Human Rights* (ECHR 1950) are binding on signatories as are decisions of the associated supranational Court where complaints of infringement are heard. In regard to privacy, Article 8 of the ECHR states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and the freedoms of others.⁸⁹

The right to privacy expressed in Article 17 of the ICCPR and Article 8 of the ECHR is significant for individuals in countries, such as Jordan, that lack domestic privacy protection laws. Individuals in Jordan may be able to claim

⁸⁸ Article 17 of the *International Covenant on Civil and Political Rights* opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976). Text avail <<http://www.hrcr.org/docs/Civil&Political/intlcivpol5.html>> at 6 November 2008.

⁸⁹ECHR art 8.

privacy protection in cases where there has been a violation in terms of these two articles. Lawmakers in Jordan may also be under a legal duty to introduce laws to protect privacy in compliance with the ICCPR (as Jordan is a signatory) and/or ECHR principles.⁹⁰

For an example of the incorporation in EU countries of the ECHR provisions, Article 8 of the ECHR has been incorporated into domestic law in the United Kingdom by the *Human Rights Act 1998* (UK).⁹¹ Neither Article 8 of the ECHR nor Article 17 of the ICCPR have been incorporated into Jordan's domestic laws by the *National Centre for Human Rights Law No 51 of 2006*⁹² although, as a signatory to the ICCPR, Jordan submits ICCPR periodic reports as required, the most recent being that considered on 23 October 2010.⁹³

On the national level, the United States and the European Union have very different conceptions of privacy. The US legal system treats privacy as a personal property right that may be disposed of as one sees best, rather than an unassailable human right.⁹⁴ The *US Constitution* does not expressly grant individuals a right to privacy.⁹⁵ In *Katz v United States*, the US Supreme

⁹⁰ Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6(3) *International Journal of Law and Information Technology* 247, 248.

⁹¹ *Human Rights Act 1998* (UK) art 8.

⁹² Nor its temporary or provisional predecessor passed in 2002. For more information, see 'Jordan: Jordan National Center for Human Rights', Asia Pacific Forum (2010) <<http://www.asiapacificforum.net/members/apf-member-categories/full-members/jordan>> at 27 November 2010.

⁹³ Human Rights Committee, *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: Fourth Periodic Report of Jordan* (CCPR/C/JOR/4; CCPR/C/JOR/Q/4 and Add.1/HRI/CORE/1Add.18/Rev.1): 100th sess, sum record of 2748th mtg, 13 October 2010 CCPR/C/SR.2748.

⁹⁴ Long and Quek, above n 13, 332.

⁹⁵ Rita Marie Cain, 'Global Privacy Concerns and Regulation - Is the United States a World Apart?' (2002) 16(1) *International Review of Law Computers & Technology* 23.

Court rejected a narrow view of privacy (that would ‘turn upon the presence or absence of a physical intrusion into any given enclosure’ and held that there is a limited constitutional right of privacy based on several provisions in the *Bill of Rights* (such as the right to privacy from government surveillance), and brought it into an era where, as the Fourth Amendment sought to ‘protect people not places’,⁹⁶ a person has a ‘reasonable expectation of privacy’ under the Fourth Amendment.⁹⁷

The US Federal Trade Commission (FTC), however, has encouraged industry leaders to adopt effective self-regulatory programs.⁹⁸ The FTC has stated in testimony before Congress on 13 July 1999 that ‘self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology.’⁹⁹

Unlike the US, the European Union recognises privacy as a fundamental human right and has adopted a comprehensive approach by introducing the *Directive on the Protection of Personal Data (EU Directive 95/46/EC)*. The comprehensive European approach to the protection of personal information is characterised by four elements. According to Paul Schwartz and Joel Reidenberg, these elements are: (a) the establishment of obligation and responsibilities for personal information; (b) the maintenance of transparent

⁹⁶ *Katz v United States*, 389 US 347 (1967) 347 (Stewart J).

⁹⁷ *Katz v United States*, 389 US 347 (1967) 360 (Harlan J).

⁹⁸ Federal Trade Commission, 'Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress' (2000) 34.

⁹⁹ Federal Trade Commission, 'Self-Regulation and Privacy Online' (1999) Testimony: Before the Subcommittee on Communications of the Committee on Commerce, Science and Transportation, US Senate, 27 July 1999. Prepared statement by the Federal Trade Commission Chairman, Robert Pitofsky <<http://www.ftc.gov/os/1999/07/privacyonlinetestimony.pdf>> at 4 March 2010.

processing of personal information; (c) the creation of special protection for sensitive data; and (d) the creation of enforcement rights and effective oversight of the treatment of personal information.¹⁰⁰

According to Peter Swire and Robert Litan, the differences between these two approaches can be referenced to the ‘different information cultures’ of the two jurisdictions.¹⁰¹ In her book review, Pamela Samuelson attributes these differences to four factors. First: Americans are generally more trusting of the private sector and the market.¹⁰² Second, Americans tend to believe in the power of the mass media to prevent the private sector from having poor privacy practices.¹⁰³ This assumes that mass media will provide consumers with information about private sector practices so that consumers can exercise their market power to shop for firms with good policies.¹⁰⁴ Third, Americans are inclined to think that technologies can contribute to the solutions of problems created by technologies.¹⁰⁵ Finally, Americans are more inclined to adopt reactive rather than proactive regulation. The US prefers to tailor regulatory solutions to problems as they appear rather than to adopt broad regulations anticipating problems yet to arise.¹⁰⁶

¹⁰⁰ Paul M Schwartz and Joel R Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996) 13.

¹⁰¹ Peter P Swire and Robert E Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998) 153.

¹⁰² Pamela Samuelson, 'Book Review: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy' (1999) 87 *California Law Review* 751, 756.

¹⁰³ *Ibid.*

¹⁰⁴ *Ibid* 757.

¹⁰⁵ *Ibid* 756–7.

¹⁰⁶ *Ibid* 757.

1.8 Chapter Outline

In addition to the current chapter, the thesis consists of another eight chapters. Here below is a brief outline of these chapters.

Chapter Two examines the meaning of privacy and why it means different things to different people. It starts with an examination of many of the attempts at defining the concept of privacy. It has been argued that one of the main problems in implementing a law of privacy is the failure to provide an accepted working definition of privacy.¹⁰⁷ Therefore, this section is important for the research question as it helps to provide to some extent a legal framework for privacy protection in Jordan. It supports the idea that privacy is a central requirement for democracy. One important conclusion of this chapter is that the adoption of greater democracy in Jordan remains incomplete due to the lack of privacy laws. The introduction of surveillance technologies without a proper legal framework could result in wholesale discrimination against and hardship for vulnerable people. Such technologies can adversely affect the delicate balance pursued by an emerging democracy. The adoption of information technology causes an imbalance in the relationship between individuals and the state.¹⁰⁸ For example, a government's eavesdropping practices will create an unpleasant and distrustful relationship between individuals and their government.

Chapter Three continues to explore the meaning of privacy as it exists in accordance with the principles of Islam. It traces the origins of privacy in the

¹⁰⁷ Moore, above n 52, 10.

¹⁰⁸ Simon Davies and Ian Hosein, 'Privacy 1: Liberty on the Line' in Liberty (National Council for Civil Liberties) (ed), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (1999) 73.

Shari'ah (Islamic law) and connects this with the current laws in order to demonstrate that the concept of privacy can further evolve in the Jordanian context. The main outcome of this chapter is that the concept of privacy is shown to be in accordance to the *Shar'iah* and indeed that it is there regarded as a fundamental human right. Some aspects of privacy have been illustrated and evidence elicited from the *Holy Qur'an* and *Sunnah* to demonstrate this position.

The next two chapters investigate current privacy practices by public and private sectors in the ICT sector. Chapter Four provides a case study on governmental initiatives related to the public sector. The study identifies privacy implications for and challenges to individuals provided by the e-government of Jordan. This chapter, with empirical data provided, criticises the lack of policies and guidelines to regulate the activities involved in this initiative in regards to privacy protection.

Chapter Five evaluates and assesses the extent to which individual privacy is protected in the private sector. An empirical study of the banking and telecommunications businesses in Jordan is conducted as they have become the largest industries to use ICTs.

Chapter Six reviews the current legal landscape of privacy protection in Jordan. It starts by briefly giving a background to the legal system in Jordan. The Jordanian legal system has two major sources of legislation: the civil law and the *Shari'ah*. The chapter then explores privacy rights within the *Constitution of Jordan*. In this regard, the *Constitution* does not provide explicit

protection to the concept of privacy. The chapter then goes on to discuss other major legislation that may be applicable to privacy.

Nevertheless, at the time of writing, the Jordanian legal system has no specific laws or regulations for individual privacy protection. The lack of such laws and regulations provides an opportunity for this thesis to examine and compare other regimes in regard to privacy protection. The intention, here, is to determine which of these regimes is achievable for Jordan. Therefore, Chapters Seven and Eight discuss in detail two of the most important regimes to privacy protection, at least from Jordan's perspective.

Chapter Seven looks in detail at the US legal landscape for privacy protection. It starts by examining the historical development of privacy regulation in the United States which regards privacy as a property right rather than a human right. With its concurrent belief in free market forces and preference for freedom from government intervention more generally, the United States believes that privacy protection can best be achieved through the implementation of self-regulatory measures rather than central legislation. The chapter summarises the current privacy laws and regulations which are applicable to businesses in the banking and telecommunications sectors.

This pro-self regulatory position of the US may have an impact on Jordanian policy-makers, persuading them to adopt a similar approach for privacy protection in Jordan. Jordan's strong relationship with the United States in

many fields may yet prove a sufficient factor to encourage the Jordanian government to implement such approach.

The following chapter then examines one of the most influential pieces of legislation in relation to privacy protection. Chapter Eight describes the impacts of the *EU Directive 95/46/EC* on countries (such as Jordan) that do not have privacy protection laws or regulation. It examines some of the most important provisions included in the Directive, namely Articles 25, 26 and 29. These provisions, and particularly Article 25, have seriously affected how other jurisdictions shape their own privacy legislation. In accordance with the Directive's provisions, organisations based in Jordan may be found not to have 'adequate' privacy protection policies. This may result in a situation where an organisation located in Europe may be prevented from sending data to its counterpart branch based in Jordan. Such a ban on transfer would create economic harm in Europe and Jordan and would 'lend credence to fears that the privacy laws are being used in a protectionist way to keep out non-European businesses'.¹⁰⁹

The final chapter (Chapter Nine) summarises the findings of this research and proposes a model legal framework for privacy protection in Jordan as a final thought. It justifies the urgent necessity for the adoption of such a model. The proposal aims to provide individual privacy protection through specific laws and regulations. In addition, the proposal recommends the

¹⁰⁹ Swire and Litan, above n 101, 17.

establishment of an independent privacy protection agency to enforce and oversee privacy rights included in the proposed legal framework.

Chapter Two

The Concept of Privacy

2.1 Introduction

One important observation stated in the previous chapter is that the Jordanian legal system does not currently provide a specific legal framework for privacy protection generally or, more particularly, in the context of the proliferation and growth of information and communications technology. A main problem for implementing such a legal framework is the lack of an accepted working definition of privacy. In order to address this problem, this chapter first examines what privacy is, and how different definitions of privacy constitute different approaches to privacy protection. The intention here, however, is not to provide a descriptive literature of all definitions of privacy and analysing it in terms of what is wrong and what is right, but rather to seek the most suitable definition of privacy for adoption by the Jordanian legal system. It aims to explore a legal concept of privacy. The first section discusses the importance of privacy in general and for Jordan in particular. It also provides brief accounts of the benefits and costs of protecting privacy.

The next section evaluates relevant international documents regarding the right to privacy. Those international instruments now recognise the right to privacy as a fundamental human right. This evaluation is significant for countries like Jordan that do not have legislation recognising and protecting the right to privacy. The international recognition of privacy as a fundamental human right (in so far as this is reflected in those international

documents and as shown in Figure 1, above) may further support the main argument that privacy should be considered a fundamental human right to be protected by legislation and regulation. The next section provides an assessment of other documents that provide privacy protection in the form of guidelines, such as the OECD and the APEC guidelines. It has been argued that these guidelines for privacy protection (generally adopted as part of a self-regulatory approach) are based on economic interests with regard to privacy protection rather than viewing it as one of a number of fundamental human rights.

2.2 Definition of Privacy

Currently, there is no consensus in the legal and philosophical literature on a definition of privacy.¹ 'Privacy' is a term used with many meanings.² According to Hyman Gross, privacy is 'the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited'.³ Gross argues that: a 'loss of privacy occurs when the limits one has set on acquaintance with his personal affairs are not respected.'⁴ Other scholars provide definitions of privacy based on the element of personal control more than on any particular personal area in which such control might become important. Robert Ellis Smith has explained this element of control by saying that:

¹ Richard B Parker, 'A Definition of Privacy' (1974) 27(2) *Rutgers Law Review* 275.

² Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89(3) *The Yale Law Journal* 421, 424.

³ Hyman Gross, 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34, 36.

⁴ Hyman Gross, 'Privacy and Autonomy' in Roland Pennock and John W Chapman (eds), *Privacy* (1971) 170.

Control ... privacy is the right to control your own body, as in the right to an abortion or the right to whatever sexual activities you choose. Privacy is the right to control your own living space, as in the right to be free from unreasonable searches and seizures. Privacy is the right to control your own identity, as in the right to be known by a name of your choice and not a number, the right to choose your own hair and dress styles, the right to personality. Privacy is the right to control information about your self, as in the right to prevent disclosure of private facts or the right to know which information is kept on you and how it is used.⁵

Charles Fried considers privacy as a form of power; he defines privacy as ‘the control over knowledge about oneself’. Therefore, ‘the only way to give a person this control is to give him a legal title to control’.⁶ Alan Westin defines privacy as ‘the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’.⁷ The most significant definition of privacy to have attracted academic and public attention is the ‘right to be let alone’.⁸ This definition was popularised by Samuel Warren and Louis Brandeis in their 1890 article, ‘The Right to Privacy’, where they argued that it was necessary for the legal system to recognise the right to privacy because when the right is violated, such as when information about an individual’s private life is made available to others, such publication may affect not only the perceptions held by others of that person and their actions towards the

⁵ Robert Ellis Smith, *Privacy* (1979) 323.

⁶ Charles Fried, 'Privacy' (1968) 77 *The Yale Law Journal* 475, 483.

⁷ Alan F Westin, *Privacy and Freedom* (1967) 7.

⁸ Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 195.

individual or group, but also affect and even injure the very core of an affected individual's personality.⁹

The above definitions, however, have been criticised. The control based definitions were criticised on their focus that sees personal information as the property of the person to whom it relates. Personal information is different from commodities.¹⁰ In addition, control based definitions fail to explain what are the types of information over which individuals should have control. According to Solove, a control of information based definition is 'too narrow a conception for it excludes those aspects of privacy that are not informational; such as the right to make certain fundamental decisions about one's body, reproduction, or rearing of one's children'.¹¹ Consequently, despite the failure to define the type of information, most people would probably regard surveillance, spying and eavesdropping as invasions of privacy regardless of whether any new information or any particular sensitive information is gained by these means.¹²

The definition of privacy as the 'right to be let alone' has also been criticised as it is simply too vague.¹³ It leaves open the questions of in what ways, and in what matters, should individuals be left alone. As Anita Allen writes:

If privacy simply meant "being let alone", any form of offensive or harmful conduct directed toward another person could be characterized as a violation

⁹ Dorothy J Glancy, 'The Invention of the Privacy' (1979) 21(1) *Arizona Law Review* 1, 2.

¹⁰ New Zealand Law Commission, *Privacy: Concepts and Issues Study*, Paper No 19 (2008) 36.

¹¹ Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1110.

¹² Judith Wagner DeCew, 'The Scope of Privacy in Law and Ethics' (1986) 5(2) *Law and Philosophy* 145, 154-8.

¹³ Solove, 'Conceptualizing Privacy', above n 11, 1102.

of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom.¹⁴

Moreover, behaviour that is not offensive or harmful could be characterised as failing to let someone alone, and the only way of being truly let alone is to live in complete isolation from society.¹⁵

In his distinguished article ‘Conceptualizing Privacy’, Daniel Solove proposed a new approach to privacy, one based on ‘understanding privacy rather than a definition or formula for privacy’.¹⁶ It is to be regarded as an approach ‘because it does not describe the sum and substance of privacy but provides guidance in identifying, analyzing and ascribing value to a set of related dimensions of practices’.¹⁷ Such an approach, as Solove points out, ‘should aid in solving problems, assessing costs and benefits in structuring social relationships’.¹⁸ This approach to conceptualising privacy is context specific, and involves examining privacy invasions as disruptions of particular practices. Such disruptions could include, for example, interference with peace of mind, intrusion on solitude, or loss of control over facts about oneself.¹⁹ Solove notes that there are similarities and differences among both the disruptions and the practices they disrupt, and contends that ‘we should conceptualize privacy by focusing on the specific types of disruption and the

¹⁴ Anita L Allen, *Uneasy Access: Privacy for Women in a Free Society* (1988) 7.

¹⁵ New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 10, 34.

¹⁶ Solove, ‘Conceptualizing Privacy’, above n 11, 1129.

¹⁷ *Ibid.*

¹⁸ *Ibid.*

¹⁹ *Ibid.*

specific practices disrupted rather than looking for the common denominator that links all of them.’²⁰

Solove suggests that ‘the landscape of privacy is constantly changing,’ particularly as a result of technological developments, and that scholars and judges may be led astray by ‘trying to fit new problems into old conceptions’.²¹ Instead,

[W]e should seek to understand the special circumstances of a particular problem. What practices are being disrupted? In what ways does the disruption resemble or differ from other forms of disruption? How does the disruption affect society and social structure?²²

The main shortcoming of his approach is that it provides no basis for establishing why some harms are privacy violations and others are not. To return to the example provided by Anita Allen (quoted above): Why is a ‘peep in the bedroom’ — but not a punch in the nose — an invasion of privacy?²³ In addition, Solove’s approach is one way of conceptualising privacy violations rather than privacy itself. His focus on harms in the form of disruption of specific practices lends itself well to a legal and policy analysis based on the prevention or remedying of harms. However, while it is a useful way of understanding privacy violations or problems, it does not greatly assist our understanding of what it means to experience privacy.²⁴

²⁰ Ibid 1130.

²¹ Ibid 1146.

²² Ibid 1147.

²³ New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 10, 41.

²⁴ Ibid 41.

An analysis of the above discussion prompts two important observations. First, it may be difficult to define precisely what privacy is, but addressing privacy problems is achievable. The concept of 'privacy' is understood or found when some particular practices occur. These practices, however, are categorised as 'violations of privacy'. In this regard, Solove's approach could be suitable for specific legal systems which lack a clear definition of privacy.

In Jordan, for instance, identifying privacy violations and problems is not less than experiencing the right of privacy itself. Attending to these violations and problems by setting up privacy protection policies in the form of laws, guidelines or other types of policies may assist in the formulation of a definition of privacy within particular areas. For example, telemarketing has been widely regarded as an intrusion on individual privacy, and is seen as violating the 'right to be let alone'. As a result, in the United States, a 'do not call' policy was introduced in June 2003 in order to prohibit telemarketing companies from calling customers who chose to have their numbers listed in a specific telephone registry. The US National Do Not Call Registry was challenged by the telemarketing industry on the basis that such a registry infringed on commercial speech by introducing unconstitutional content-based restriction and such an intrusion lacked legal authority. However, these challenges were dismissed on the grounds that the Registry has a legitimate and substantial interest in protecting citizens' privacy in terms of the right to be left alone in their own homes.²⁵ The National Do Not Call

²⁵ William G Staples (ed), *Encyclopedia of Privacy* (2007) 178.

Registry has as of December 2009 over 191 million active numbers.²⁶ This is an example of how individuals can experience their privacy rights in one particular area. The right of privacy in this context is the right ‘not to be called’.

Second, the difficulty of providing a clear definition of the concept of privacy has led scholars to produce many different accounts and statements of the benefits and costs of privacy. However, the author believes that ‘information control based’ definition of privacy is appropriate for the Jordanian legal system and should be adopted under Jordan legislation dealing with privacy issues. Therefore, in the thesis privacy or ‘informational privacy’ may be defined as ‘the individual’s ability to control the circulation of information relating to him’.²⁷ Privacy is ‘the right to control when, how and by whom personal information about oneself is communicated to and used by others’.²⁸ This thesis considers the term ‘personal information’ as having the same meaning as the definition provided by Australian Law Reform Commission (ALRC), which is ‘information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual’.²⁹

²⁶ Federal Trade Commission, 'Biennial Report to Congress: Pursuant to the Do Not Call Registry ' (2009) 1 <<http://www.ftc.gov/os/2010/01/100104dncbiennialreport.pdf>>.

²⁷ Arthur Raphael Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (1971) 40.

²⁸ Sandra Byrd Petersen, 'Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?' (1995) 48 *Federal Communications Law Journal* 163, 164.

²⁹ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 309.

This section has dealt with the conception of privacy. The next section examines the significance of privacy and provides a justification as to why the definition of informational privacy should be adopted.

2.3 Importance of Privacy

Opinions differ in regards to the interests and values that are protected by a right to privacy.³⁰ Much of the scholarly literature agrees to some extent that privacy has social and economic importance. The respect for privacy enriches social and personal interaction by providing contexts for the development of various kinds of relationships and multiple dimensions of personality.³¹ In his remarkable book *Privacy and Freedom*, Alan Westin examines the significance of privacy for individuals and groups in democratic states. According to Westin, privacy performs the following functions: (1) personal autonomy — satisfying ‘the human desire to avoid being manipulated or dominated by others’;³² (2) emotional release — performing ‘a protective function at moments of less intense stress, during the periods of anxiety and uncertainty which are part of daily life’;³³ (3) self-evaluation — privacy fulfils individual needs by providing opportunity for people to integrate their experiences into a meaningful pattern and exert their individuality on events;³⁴ and (4) opportunity for limited and protected communications — privacy provides

³⁰ Barbara von Tigerstrom, 'Protection of Health Information Privacy: The Challenges and Possibilities of Technology' (1998) 4 *Review of Current Law and Law Reform* 44, 46.

³¹ Ferdinand Schoeman, 'Privacy and Intimate Information' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 413.

³² Westin, *Privacy and Freedom*, above n 7, 33.

³³ *Ibid* 36.

³⁴ *Ibid*.

‘room’ to share candid communications, confidences and intimacies with trusted persons’.³⁵

Furthermore, Ruth Gavison argues that privacy is needed to enable a person to deliberate upon and establish his/her views and opinions. If public reaction seems likely to be unfavourable, privacy will allow this person to express his/her judgements to a group of like-minded people. After a period of development within that limited privately shared space, such a person may be more willing to declare their unpopular views and opinions without fearing public reaction.³⁶

Gavison further argues that privacy promotes liberty in ways that enhance the capacity of individuals to create and maintain human relations at different intensities. It helps individuals to continue relationships, while feeling free to endorse those feelings in private.³⁷

Gavison goes to claim that ‘privacy has a role to play in politics because it fosters and encourages the moral autonomy of the citizens, a central requirement of a democracy’.³⁸ A country might restrict certain activities, but it must allow some liberty of political activities if it is to retain its status as a democracy. Gavison states:

This liberty requires privacy, for individuals must have the right to keep private their votes, their political discussions and their associations if they are

³⁵ Ibid 38. See also (in regard to the functions of privacy), Alan F Westin ‘Science, Privacy and Freedom: Issues and Proposals for the 1970s: Part 1 – The Current Impact of Surveillance on Privacy’ (1966) 66 *Columbia Law Review* 1003, 1022-8.

³⁶ Gavison, above n 2, 450.

³⁷ Ibid 450.

³⁸ Ibid 455.

to be able to exercise their liberty to the fullest extent. Privacy is crucial to democracy in providing the opportunity for parties to work out their political positions, and to compromise with opposing factions, before subjecting their positions to public scrutiny. Denying the privacy necessary for these interactions would undermine the democratic process.³⁹

The above statement is indeed provides a supportive discussion to explain the current situation in Jordan. One of the reasons that prevent democratic development in Jordan is that people do not have 'personal autonomy'. Since the foundation of Jordan as an independent state, there has been a relationship of dependency between the Government of Jordan and its citizens. Citizens rely on the government to provide them with basic needs.

However, this relationship has never been based on trust being extended to the government by the people but rather based on fear and a lack of alternatives. People have no other channels but the central Government to fulfill their requirements. As a result, citizens fear expressing their personal political, economic and social views. In a 2007 poll conducted by the Centre for Strategic Studies of the University of Jordan, 78 per cent of respondents stated that they could not publicly criticise or express their disagreement with the government without exposing themselves and their family members to persecution in terms of their security or livelihood. Eighty-two per cent of those respondents believed that they would expose themselves and their family members to security related issues if they participate in peaceful political opposition activities, such as demonstrations and pamphlet

³⁹ Ibid 456.

distribution, or wrote articles, or participated in conferences, workshops, and political opposition forums.⁴⁰

With respect to the above poll, the author believes that privacy laws would help to establish and maintain the right of expression and the right of speech in Jordan. A good example to support this view of the need for privacy is found in the use of the electronic media in Jordan. Individuals, who place their comments on electronic media websites regarding local and/or international news and reports, would refuse to provide their truthful personal information fearing that this information may be passed to third parties.

In this regard, Professor Roger Clarke argues that the right of privacy has in terms of its psychological, sociological, economic and political dimensions. These dimensions can be elaborated as follows:

Psychologically: people need private space. This applies in public as well as behind closed doors and drawn curtains...

Sociologically: We need to be able to glance around, judge whether the people in the vicinity are a threat, and then perform actions that are potentially embarrassing, such as breaking wind, and jumping for joy.

Economically: people need to be free to innovate. International competition is fierce, and countries with high labour-costs need to be clever if they want to sustain their standard-of-living. And cleverness has to be continually reinvented. But the chilling effect that surveillance brings with it stifles innovation. All innovators are, by definition, 'deviant' from the norms of the

⁴⁰ Faris Braizat, 'Democracy in Jordan 2007' (Centre for Strategic Studies-University of Jordan, 2007) 10, avail <<http://www.css-jordan.org>> at 22 April 2009.

time, and they are both at risk, and perceive themselves to be at risk, if they lack private space in which to experiment.

Politically: people need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and undermines democracy.⁴¹

A lack of anonymity (which involves the right to control disclosure of one's identity in particular circumstances) may facilitate one of the most common forms of corruption found in Jordan, that is, 'favouritism'. This type of corruption is widely accepted and deeply rooted in Jordanian society. It can affect admission to universities, receipt of good marks at school, public service recruitment and promotion,⁴² even accessing a bank loan or financial support from the government, as well as the granting of tax exemptions or even an acquittal at court.⁴³ Here perhaps an argument could be made for the establishment of stricter guidelines to preserve the privacy of a person's identity and ensure that a person's name/identity — a factor irrelevant to examinations, university admission (for example) — does not affect outcomes. The privacy of student/applicant's name could be maintained by the simple use of numerical identifiers in examinations in order to restrict favouritism (and its opposite persecution). Results could at least be evaluated and tallied on the basis of performance rather than 'name' or affiliation of a student, candidate and so forth. Across Jordanian society the idea of informational 'privacy' as a right and its role in a just society needs to be broadly publicised and recognised. Even elections can currently be affected

⁴¹ Roger Clarke, *What's 'Privacy'?* (2006) <<http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html>> at 2 June 2009.

⁴² Markus Loewe, Jonas Blume and Johanna Speer, 'How Favoritism Affects the Business Climate: Empirical Evidence from Jordan' (2008) 62(2) *The Middle East Journal* 259, 268.

⁴³ *Ibid* 264.

— the mutual expectations of electors and elected maintain an atmosphere where favouritism flourishes. Here the privacy of the voters and their voting intention is violated for mutual gain in a manner that would not be tolerated in a modern democratic society and should not be tolerated in Jordan as it becomes such a country. A few words of explanation are needed for those unfamiliar with the Jordanian context. The primary goal of voters in Jordan (as is often the case elsewhere to some degree at least) is personal gain. In Jordan, however, the relationship is far more direct. Electors expect their MP to provide them with jobs, services, and information on profitable business opportunities. Many MPs predominantly pursue the narrow interests of particular constituents, rather than design and decide on reforms that serve the country as a whole.⁴⁴ To again or maintain power, a candidate asks voters to supply their personal documents (such as their national identification card) which is returned only after election day. Voters agree to such practice in return for service and benefits if their candidate wins the election. Such an arrangement promotes narrow sectorial interests, perhaps to the detriment of the broader community. This type of practice represents a violation of what should be a matter of individual privacy (even if mutually agreed) and corrupts the voting process. Again legislation outlawing the practice should be introduced and rigorously enforced. This could facilitate an electoral process where voters are free to express their views privately in the ballot box.

⁴⁴ Ibid 269.

Privacy in the ballot box is just one area which must be sacrosanct for the creation and maintenance of a healthy democracy. Again electors' ability to express their opinions far more freely via email either to likeminded individuals or more publicly in the internet webpages, blogs and so forth, needs to be protected for genuine democracy to flourish. E-surveillance, as mentioned earlier, where people's identities and associated transmissions and so forth are routinely monitored and disclosed to government, is not conducive to the freedom of expression — even in private communications or to a small group of like-minded individuals or to society at large in an pseudo-anonymous communiqué — that is necessary for growth and change.

As Clarke notes above, freedom and privacy of communication is also necessary for economic development. While he appears to mention it in the context of highly developed western high-wage economies, privacy is surely equally required for inventors and innovators in rapidly developing societies such as Jordan. Privacy and intellectual freedom are inextricably linked. Economic benefits flow from local and international innovations possible in such a context.

The author strongly believes that privacy is significant for achieving the psychological, sociological, economic, and political benefits mentioned above. It gives individuals the ability to create new opportunities and develop new ideas that may benefit society and the economy as a whole. It also plays vital role in the development and maintenance of individual identity. Information privacy plays a significant role as a boundary control process for defining this

identity through interactions with others.⁴⁵ The only way for individuals to conceive this identify is when they feel liberated from being controlled by others. In addition, the above mentioned forms of corruption, which, among other factors, are due to the lack of privacy laws, will discourage many from being creative in their own society and deny them opportunities in education, or in the workplace, or restrict their capacity to participate either politically or economically in a society that requires the best possible person for each and every position. Privacy legislation and privacy protection are a necessity for Jordan's continued development. A proliferation of privacy is not without its risks, however, as the following reveal.

The broad variation regarding the role and value of privacy has led some scholars to question its real value. Robert Post has lamented that:

Privacy is a value complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.⁴⁶

Giving people privacy can result in harm to society. People could exaggerate their personal achievements or otherwise distort many personal truths about themselves. For example, without access to accurate unbiased records, employers will be worse placed in relation to ascertaining the most suitable job candidate. Without accurate information, credit providers would be unable to make more informed business decisions.⁴⁷

⁴⁵ Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (2005) 45.

⁴⁶ Robert Post, 'Three Concepts of Privacy' (2001) 89(6) *Georgetown Law Review* 2087.

⁴⁷ Doyle and Bargaric, above n 45, 44.

In addition, privacy can be an essential ingredient of criminality and provides the environment in which wrongdoers can engage in conduct such as theft, robbery, rape, murder and reckless driving which directly violates the capacity of others to lead their lives in their chosen manner.⁴⁸

Moreover, recognising a right to privacy from an economic perspective would likely increase direct and indirect cost to the individual. For example, targeted offers reduce marketing and distribution costs for sellers, and thus ultimately reduce the prices of all goods and services. Auctions, reverse auctions and other pricing innovations that make it easier for buyers and sellers to exchange information not only reduce online prices but also create competitive pressures that also reduce offline prices.⁴⁹

Judith Jarvis Thomson argues that privacy is neither distinctive nor useful. Privacy according to Thomson is not a coherent concept in itself, but rather a 'catch-all' that reduces, in various cases, the complex to more primitive concepts that are more easily understood such as property, contracts and bodily rights.⁵⁰ Therefore, Thomson recommends abandoning the search for a coherent concept of privacy in favour of focusing on less contentious rights, especially property rights and rights over the person.⁵¹ However, Thomson's argument has been criticised on two main grounds. First, her argument is based on a very broad view of what is encompassed by property rights and rights over the person. Her concept of 'the right over the person' includes the

⁴⁸ Ibid.

⁴⁹ Kent Walker, 'The Cost of Privacy' (2001) 25 *Harvard Journal of Law and Public Policy* 87, 90.

⁵⁰ Judith Jarvis Thomson, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295, 303-10.

⁵¹ David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131, 145.

right neither to be looked at nor to be overheard. Second, even if privacy rights are derivative, it does not mean that claims to privacy rights are incoherent.⁵²

As Jeffrey Reiman notes:

Even if privacy rights were a grab-bag of property and personal rights, it might still be revealing, as well as helpful, in the resolution of difficult moral conflicts to determine whether there is anything unique that this grab-bag protects that makes it worthy of distinction from the full field of property and personal right.⁵³

The primary point concluded from the above discussion is that privacy has been widely recognised as a value important to both individuals and society. This recognition, however, has been unsuccessful in converting the value into a clearly defined, protectable legal standard.⁵⁴ Ruth Gavison suggests, that for privacy to be recognised by any legal system, it ‘must be a concept useful in legal contexts, a concept that enable to identify those occasions calling for legal protection, because the law does not interfere to protect against every undesirable event.’⁵⁵ As a result, one question has emerged: ‘Is there a legal right to privacy?’ The following section examines two opposing views, each one of which has shaped its own legal system to suit a particular view. One view is that the legal protection to privacy is based on the concept of property rights. The contrasting view recognises privacy as a fundamental human right.

⁵² Ibid.

⁵³ Jeffrey H Reiman, 'Privacy, Intimacy and Personhood' (1976) 6 *Philosophy and Public Affairs* 26, 28.

⁵⁴ Priscilla M Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (1995) 41.

⁵⁵ Gavison, above n 2, 423.

2.4 Privacy as a Legal Concept: Property Right or Human Right?

The right to informational privacy is considered a right of property. Alan Westin suggests that ‘personal information, thought of as decision over one’s private personality, should be defined as a property right.’⁵⁶ The individuals entitled to the benefits of information being described as its owners⁵⁷ would retain ownership in their personal information and have the right, but not the obligation, to sell this information.⁵⁸ Personal information defined as property means that the individual holds the right for commercial exchange of his/her information privacy in the marketplace. Businesses interested in data acquisition can then offer a price to the consumer in exchange for their information.⁵⁹ The essential principle, however, is that no information could legally be sold or traded without the express permission of the person who owns the right of property over his/her personal information. Such a right would constitute no obstacle to any organisation’s maintenance of any records of personal information collected from such person.⁶⁰ Personal information in this case is no longer the property of the person concerned; it could be sold or transferred to third parties without obtaining his/her consent.

⁵⁶ Westin, *Privacy and Freedom*, above n 7, 324.

⁵⁷ Allison Coleman, *The Legal Protection of Trade Secrets* (1992) 48.

⁵⁸ Kenneth C Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information* (1997) US Department of Commerce, avail at <<http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy>> at 22 July 2009.

⁵⁹ Detlev Zwick and Nikhilesh Dholakia, 'Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right' (2001) 11(2) *Electronic Markets* 116, 118.

⁶⁰ James Rule and Lawrence Hunter, 'Towards Property Rights in Personal Data' in Colin J Bennett and Rebecca Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (1999) 170.

The US is considered to be the best example of this view. Personal information under the US law is treated as a property right rather than fundamental human right. The US applies the market-based approach in dealing with any issues concerning informational privacy.

Consequently, rather than address the concept of privacy ‘across the board’ in a single piece of legislation with sections dealing with its various manifestations, information privacy laws in the US have been enacted on an ad hoc basis, that is, a number of separate laws have been enacted, each addressing particular issues. Legislation has been enacted to deal with problems as they have arisen in specific sectors (such as financial institutions), or in regard to specific practices (such as direct-marketing), and in relation to specific types of information. Examples include the *Fair Credit Reporting Act of 1970*⁶¹ was enacted only to address consumer credit information while the *Electronic Communication Privacy Act of 1986*⁶² was enacted to address privacy issues concerning electronic communications content. The same piecemeal approach is adopted in the enactment of other privacy laws to address issues related to medical information, and driver information.⁶³ These laws, among others, will be discussed in detail in Chapter Seven.

This approach is justified on the grounds that the US promotes the free flow of information which assists, in turn, in promoting commerce and providing citizens with significant economic and social benefits. In addition, this

⁶¹ 15 USC § 1681 (1970).

⁶² 18 USC § 2510 (1986).

⁶³ Lindsay, above n 51, 168.

approach provides a more effective and sensitive means of protecting personal privacy (in terms of facilitating specifically targeted protection in certain sectors of businesses).⁶⁴ This approach, however, is examined in more detail in Chapter 5 when discussing the US approach to privacy.

Another view considers privacy as a fundamental human right. Legal protection of information privacy is seen as a necessary condition for citizenship, as well as being necessary for the development of a desirable society.⁶⁵ From this perspective, in treating privacy as a fundamental human right, privacy is:

categorised as inalienable; in the same manner that the right to vote may not be traded or that organs may not be sold. The operative notion is that personal information is so intimately bound up with individual integrity and autonomy that it should not be permissible to bargain it away.⁶⁶

Therefore, personal information is not to be ‘owned’ as much as protected against repressive state power as well as greedy business practices. As a result, privacy is irreducible to the individual property principle and personal information cannot be commodified.⁶⁷

This rights-based view has been adopted by the European Union in its enactment of the most influential privacy legislation, the *European Union*

⁶⁴ James M Assey and Demetrios A Eleftheriou, 'The EU-US Privacy Safe Harbor: Smooth Sailing or Troubled Waters?' (2001) 9 *CommLaw Spectus* 145, 150.

⁶⁵ Lindsay, above n 51, 169.

⁶⁶ Deborah Hurley, *A Whole World in One Glance: Privacy as a Key Enabler of Individual Participation in Democratic Governance* (2000) 5 (n 12) <<http://www.pcpd.org.hk/english/infocentre/files/hurley-paper.doc>> at 4 February 2010.

⁶⁷ Zwick and Dholakia, above n 59, 119.

Directive 95/46/EC.⁶⁸ As discussed in more detail in Chapter Eight, the Directive is a comprehensive regulation on information privacy. It regulates activities dealing with information privacy, including collecting and using information, as well as regulating the transfer of personal information to the countries that do not have adequate privacy protection laws. The Directive considers the United States a country lacking an adequate level of protection for personal information, due to the absence of privacy legislation in the US. As a result, policy makers on both sides of the Atlantic had to come up with a compromise agreement on this particular issue. The so-called US-EU *Safe Harbour Framework Agreement*⁶⁹ was introduced in 2000 to narrow the gap between the two regimes. This agreement states that consumers must be notified about the purposes for which the company collects and uses information about them. In addition, individuals must be given the opportunity to choose whether (and how) the personal information they provide is used by or disclosed to a third party.

The Agreement — as discussed in greater detail in Chapter Eight — is voluntary and only for those companies who wish to join this agreement. Rather than compel all US businesses (whether or not trading in Europe) to comply with the EU Directive, the Agreement provides a way for US companies wishing to trade with entities in the EU to ‘avoid experiencing interruptions to their business dealings with the EU or facing prosecution by

⁶⁸ Directive 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 [1995] *OJ L 8/1*.

⁶⁹ The documents that constitute the US-EU Safe Harbor Framework are available at <http://export.gov/safeharbor/eu/eg_main_018493.asp> at 5 July 2008.

EU authorities under European privacy laws,⁷⁰ this Agreement allows businesses to certify that their individual business comply with seven Safe Harbour principles. These principles are: (1) Notice, (2) Choice, (3) Onward Transfer (Transfer to Third Parties), (4) Access, (5) Security, (6) Data Integrity, and (7) Enforcement.

The author believes that the Safe Harbour Agreement is based on economic justifications to protect privacy as a property right rather than as a fundamental human right. It allows the US to maintain its legislative stance in regards to informational privacy for businesses generally without hampering the opportunities for those companies wishing to trade with UE businesses. By restricting its scope to those wishing to trade with the EU and ensuring that its participation is voluntary, the agreement limits ramifications for business and informational privacy more widely in the US and offers a simpler and inexpensive means of complying with the adequacy requirements of the EU Directive, which may benefit participating US businesses.

In the context of Jordan, the nation's *Constitution*⁷¹ specifically recognises a limited right to privacy. It only protects two aspects of individual privacy: personal freedom and privacy at home. It stipulates that 'Personal Freedom is protected',⁷² and 'dwelling houses shall be inviolable and shall not be entered except in the circumstances and the manner prescribed by law'.⁷³ These

⁷⁰ American Institute of CPAs, *Safe Harbor Agreement* avail <<http://www.aicpa.org>> at 2 April 2011.

⁷¹ *Constitution of the Hashemite Kingdom of Jordan, 8 January 1952* (Jordan)

⁷² *Ibid* art 7.

⁷³ *Ibid* art 10.

Articles can be directly traced to the *Shari'ah* (Islamic law) which views privacy as a fundamental human right. In spite of the Jordanian legal system being founded on the *Shari'ah*, it fails to explicitly recognise the right to privacy. This failure is noticeable in the absence of any current privacy legislation being implemented in accordance with the Constitution and/or *Shari'ah* (Islamic Law). However, the current situation in Jordan in regards to informational privacy seems to favour the view that personal information is to be treated as a property right. For example, the *Credit Information Law No 15 of 2010* allows credit providers to exchange history reports about individuals with other credit providers.⁷⁴ Although there is no licensed company to provide such reports at the time of writing, this law could constitute explicit evidence that the right to privacy is to be regarded as a legal concept based on property rights, particularly as such information exchange is usually predicated on a financial benefit for the entity supplying the information.⁷⁵ This law shall be further explored when discussing privacy protection in the financial sector in Jordan.

The view taken by the author is that Jordan should develop its own privacy approach, based on privacy as a human right and taking into account its own social, and economical factors, rather than importing approaches designed for certain countries, and for specific situations. Socially, Jordan is not similar to the US. As Jordan is a predominantly Muslim country, and one with Islam recognised as the State religion since the foundation of the Kingdom in 1921,

⁷⁴ *Credit Information Law No 15 of 2010, (Jordan) [Arabic] Official Gazette* No 5034, 1 June 2003, 3071.

⁷⁵ *Credit Information Law No 15 of 2010* (Jordan) art 13.

Shari'ah principals play a large part in Jordanian society. Any attempt to alter some of these *Shari'ah* principles, may have its own disastrous consequences in terms of social stability.

From an economic perspective, in comparison with the US, Jordan is a very small developing economy. The adoption of a US approach to privacy by Jordan may add additional burdens to the economy rather than enhance it. For example, it was thought that the privatisation of Jordan's public sector would enhance the economy, when in fact, turns out to be a costly process and added a huge debt to the country. While the US economy has the ability to absorb economic shocks, Jordan's economy will be impacted for many years to come.

2.5 Privacy and Other Concepts

It has been concluded from the above literature that there is no one definition of privacy. One reason for this conclusion is that the term 'privacy' can be confused or mixed with other concepts, such as secrecy, confidentiality, security and reputation. It may be useful to compare the differences in meaning between these terms and 'privacy' in order to determine if the violations or problems that may arise are privacy related or not.

2.5.1 Privacy and Secrecy

A 'secret' can be defined as something that is intentionally withheld or kept hidden by one or more social actor(s) from the scrutiny by others, and the secrecy refers to the methods and practices of such concealment. Secrecy and privacy can create confusion because secrecy also offers protection for

privacy. The distinction between secrecy and privacy can be summarised as follows:

- Privacy is generally seen as applying only to individuals; by contrast, groups, organizations and governments can have secrets and maintain secrecy. As a result, secrecy need not relate to personal information: there can be military secrets or trade secrets that do not include information about particular individuals.
- Secrecy does not necessarily protect information because of its private or intimate nature. Information may be kept for a wide range of reasons: for example, because the information could be dangerous, or could be used by others to their own advantage if revealed more widely.

Secrecy tends to convey a stronger sense of boundaries, and of being either on the inside or the outside, than privacy. A secret is generally seen as something that should not be divulged, except under specific conditions or circumstances, whereas a private matter is something that the person to whom it relates may choose to disclose.⁷⁶

For example, information held by the Ministry of Defence relating to Jordan's military information is not private, but secret. Persons — including those authorised by law to conceal such secrets — who disclose or share this information may be prosecuted in accordance with the law. Articles 3 and 6 of Jordan's *Protection of State Secrets and Documents Law No 51 of 1971* in Jordan categorises as 'Very Secret' that information which may cause harmful consequences to the State if someone discloses it, and as 'Secret' that information which does not pose any danger to the State's national interest.⁷⁷ Persons who violates this law, can be prosecuted based on the concept of revealing secretes rather than invasion of privacy.

⁷⁶ New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 10, 48.

⁷⁷ *State Secrets and Documents and Protection Law No 50 of 1971*, *Official Gazette* No 2315, 1 August 1971, 1164, avail [in Arabic] <www.lob.gov.jo> at 20 March 2009.

2.5.2 Privacy and Confidentiality

There is a fine distinction between the concepts of 'privacy' and 'confidentiality'. The term 'confidential' applies to situations in which one party has entrusted information to the other on the understanding that it will not be disclosed further.⁷⁸ Privacy, however, is a much broader concept than confidentiality, because it entails restrictions on a wide range of activities relating to personal information: its collection, retention, use and disclosure.⁷⁹ Privacy tends to be regarded as an 'aura' surrounding individuals, whereas confidentiality affixes itself to information and classifies it according to its nature and manner of communications.⁸⁰ Confidentiality only comes into play after the information in question has been obtained by a company, organisation or government (data users). Data users are expected to be responsible for the safekeeping of the personal information entrusted to them. In this sense, they have a custodial obligation to protect the information in their care.⁸¹ Confidentiality in this context is a managerial responsibility. It concerns the problems of how to manage data by rules that are satisfactory to both the managers of data banks and the individuals to whom the data pertain.⁸² However, obligations to keep information confidential can be extended to a number of situations, such as obligation of confidence between an employer and his employees, former employees, and

⁷⁸ New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 10, 49.

⁷⁹ Ann Cavoukian, 'The Promise of Privacy-Enhancing Technologies: Applications in Health Information Networks' in Colin J Bennett and Rebecca Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (1999) 116, 121.

⁸⁰ Greg Tucker, *Information Privacy Law in Australia* (1992) 5.

⁸¹ Cavoukian, above n 79, 121.

⁸² Calvin Gothlieb, 'Privacy: A Concept Whose Time Has Come and Gone' in David Lyon and Elia Zureik (eds), *Computers, Surveillance, and Privacy* (1996) 156, 156.

independent contractor.⁸³ An obligation in regard to confidentiality can also be between lawyers and their clients, or medical doctors and their patients, and so on.

The difference between the privacy and the confidentiality is crucial, because once personal information is collected, it may be too late to guarantee its protection by trying to keep it confidential. It is impossible for anyone to give an ‘ironclad’ assurance about its control or safekeeping.⁸⁴ For example, the confidentiality provisions of the Jordanian Banking Law require — in the case of a merger of banks — that the persons who seek the merger be personally responsible and legally accountable for maintaining the confidentiality of all information to which they might have access.⁸⁵ The confidentiality provision will be breached if they disclose such information. However, the provisions of this law make no reference to privacy of information whatsoever. Consequently, disclosing bank information *by a third party* cannot be considered as a breach of confidence or as a violation of privacy in accordance with this law. The author’s view is that it is required to address this loophole in the Jordanian Banking Law concerning the protection of banking information held by the third parties.

⁸³ Coleman, above n 57, 29.

⁸⁴ Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (1997) 30.

⁸⁵ *Banking Law No. 28 of 2000* as amended by *Temporary Law No.46 of 2003* art 83, *Official Gazette* No 4448, 1 August 2000 <www.lob.gov.jo> at 02 March 2009. Text avail <www.cbj.gov.jo> at 2 March 2009.

2.5.3 Privacy and Reputation

The similarity between privacy and reputation is that an attack on a person's honour and reputation is an attack on his/her right to privacy. This similarity has been recognised in most international human right instruments as will be discussed in details below. Daniel Solove has described 'reputation' as the one of the most cherished assets that someone could have.

In his book, *The Future of Reputation*, Solove states that:

Our reputation is an essential component to our freedom, for without the good opinion of our community, our freedom can become empty. Our reputation can be a key dimension of our self, something that affects the very core of our identity. Beyond its internal influence on our self-conception, our reputation affects our ability to engage in basic activities in society. We depend upon others to engage in transactions with us, to employ us, to befriend us, and to listen to us. Without the cooperation of others in society, we often are unable to do what we want to do. Without the respect of others, our actions and accomplishments can lose their purpose and meaning. Without the appropriate reputation, our speech, though free, may fall on deaf ears. Our freedom, in short, depends in part upon how others in society judge us.⁸⁶

The author, commenting on the above statement, believes that part of protecting the right to privacy is by defending someone's reputation. In some countries, like Jordan, the value of reputation represents an important part of an individual's identity. Any acts that would diminish someone's reputation will have significant impacts on every aspect of his/her life. Under the *Penal Code No 16 of 1960* of Jordan, personal reputation is protected against three types of acts: libel, slander and contempt. The provisions of this law are discussed in detail in Chapter Six.

⁸⁶ Daniel J Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (2007) 30–1.

In the context of ICT, protecting one's reputation is becoming ever more difficult and stressful due to a number of specific difficulties, including: 'technology as the publisher', 'republishing' and 'jurisdictional issue'. Therefore, the protection of one's reputation has never been so important than it is now, and its importance is likely to continue to escalate.⁸⁷ At this point, it is beyond the scope of this research to examine these difficulties facing reputation in the context of the ICT.

2.5.4 Privacy and Security

There is clearly a relationship of dependency between 'security' and 'privacy', but it is not symmetrical. While one must have security to ensure privacy, by no means does having secure infrastructure guarantee privacy.⁸⁸ Security is the tool which may be used to ensure privacy, secrecy, confidentiality and reputation. In terms of data access, it focuses on how the rules of data access established by management can be enforced, through the use of passwords, cryptography, and like techniques.⁸⁹

The full spectrum of data security, computer and network security, physical security and procedural controls must be deployed to protect personal information from a wide range of threats: inadvertent or unauthorised disclosure, intentional attempts at interception, data loss, destruction or modification, and attempts to compromise data integrity and reliability.⁹⁰

⁸⁷ 'Dan Jerker B Svantesson, 'The Right of Reputation in the Internet Era' (2009) 23(3) *International Review of Law Computers and Technology* 169, 176.

⁸⁸ Anup K Ghosh, *Security and Privacy for E-Business* (2001) 189.

⁸⁹ Gothlieb, above n 82, 156.

⁹⁰ Cavoukian, above n 79, 121.

For example, sensitive health data may be stored on computer software and protected by physical security standards preventing general entry into the area, together with logical security standards which are designed to restrict unauthorised entry into the computer software itself. Personal identification numbers or biometric security devices are examples of logical security standards.⁹¹

It was important, as discussed above, to distinguish privacy concept from the other concepts. The author believes that the concept of privacy is unique in that it provides a broader meaning than the other concepts discussed. It means honour and reputation when it relates to women or someone's family. Privacy means keeping information confidential and secure from being accessed by unauthorised personnel. In contrast, ensuring security measures for personal information does not necessarily guarantee a person's privacy is protected. The best example can be given in this context is the famous 'WikiLeaks' case. A breach of security had led to the disclosure of a large amount of information. Some of this information is related to personal information concerning world leaders' private activities and certainly subject to confidentiality and even secrecy provisions.⁹²

2.6 International Recognition of the Right to Privacy

The importance of privacy as a human right is reflected in many international human right instruments. This section examines these

⁹¹ Tucker, above n 80, 6–7.

⁹² Aljazeera, *US Candid Views on World Leaders: US State Department Documents Released by Whistle-Blowing Website WikiLeaks Provide Candid Views on Foreign Leaders* (2010) <<http://english.aljazeera.net/indepth/spotlight/usembassyfiles/2010/11/2010112820116740589.html>> at 15 December 2010.

documents to discern support for the view of privacy as a fundamental human right.

2.6.1 Universal Declaration of Human Rights (UDHR (1948), Article 12)

The Universal Declaration of Human Right (UDHR) is a declaration adopted by the General Assembly of the United Nations on 10 December 1945. It applies to all members of the United Nations.⁹³ Article 12 of the Declaration deals expressly with privacy, it provides:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, *nor to attacks upon his honour and reputation*. Everyone has the right to the protection of the law against such interference or attacks.⁹⁴

The concept of individual privacy has been here extended to include the kinship 'zone' of the family. The physical zone of protection includes the home, and correspondence with others, which may go very far from the physical home.⁹⁵ However, the rights enunciated in the UDHR have been invoked, frequently verbatim, under a number of UN, regional and bilateral human rights treaties, and under national legislations and constitutions of international organisations.⁹⁶

⁹³ Jordan has been a member of the United Nations since 14 December 1955. See United Nations Website, avail at <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en> at 15 December 2010.

⁹⁴ *Universal Declaration of Human Rights*, 10 December 1948, GA Res 217 (III) UN GAOR, 3rd sess, 183 plen mtg, UN Doc A/810 (10 December 1948), art 12 (emphasis added): UDHR <<http://www.udhr.org/UDHR/>> at 6 November 2008.

⁹⁵ James Michael, *Privacy and Human Rights: An International and Comparative Study, with special Reference to Developments in Information Technology* (1994) 19.

⁹⁶ George E Edwards, 'International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy' (2001) 26 *The Yale Journal of International Law* 323, 392.

2.6.2 International Covenant on Civil and Political Rights (ICCPR (1976) Article 17)

Privacy has been expressed internationally as a human right. Article 17 of the ICCPR to which Jordan⁹⁷ is a party, states:

1. No one shall be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, nor to *unlawful attacks upon his honour and reputation*.
2. Everyone has the right to the protection of the law against such interference or attacks.⁹⁸

In its comparison of both Article 12 of the UDHR and Article 17 of the ICCPR, the New Zealand Law Reform Commission observes that it seems that

‘the protection provided to “privacy” under Article 17 is presumably more comprehensive than that enjoyed by one’s “honour and reputation”, as no individual is to be subjected to either ‘arbitrary or unlawful interference with his privacy, family, home or correspondence’ whereas the prohibition applies only to “unlawful attacks” on one’s “honour and reputation”’.⁹⁹

Article 17 includes terms such as ‘family’, ‘home’, ‘correspondence’ and ‘unlawful’ for which it is important that these be given a broad interpretation. The term ‘home’ in English — ‘*manzel*’ in Arabic — means not only a place where a person resides, but also the place where the person carries out his/her usual occupation.¹⁰⁰ ‘Correspondence’ needs a broad interpretation and today covers, in addition to written letters, all forms of

⁹⁷ Jordan ratified the *International Covenant on Civil and Political Rights (ICCPR)* on 28 May 1975. See UNHCHR <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en> at 15 December 2010.

⁹⁸ *International Covenant on Civil and Political Rights*, art 17, (emphasis added) avail <<http://www.hrcr.org/docs/Civil&Political/intlcivpol5.html>> at 6 November 2008.

⁹⁹ New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 10, 160.

¹⁰⁰ Edwards, above n 96, 394.

communications over distance, by telephone, telegram, telex, telefax and internet (electronic mail, chat, and blogs). The most common forms of interference in this area are secret state surveillance measures (such as opening mail, metering and tapping of telephone calls) for the purpose of preventing crime and combating terrorism.¹⁰¹

With respect to the term 'family', it also needs to be interpreted in a broad sense, taking into account various cultural and religious traditions.¹⁰² In addition to blood relationship and statutory forms of establishing relations (marriage, adoption), other criteria such as living together or economic ties that are essential for the existence of a family may define what is meant by 'family'. In the context of the right to privacy, respect for family life means primarily that the state should not arbitrarily interfere with the family's internal operations and relations, or by dividing it, by, for example, summarily separating children from their parents.¹⁰³

Additionally, the term 'unlawful' means that no interference can take place except in circumstances envisaged by the law. Interference authorised by states can only take place on the basis of law, which itself must comply with

¹⁰¹ Manfred Nowak, 'Civil and Political Rights' in Janusz Symonides (ed), *Human Rights: Concept and Standards* (2000) 89.

¹⁰² For instance, in the United Kingdom, transgender matters and homosexual acts fall under the right to privacy. See Your Rights, IN FULL <<http://www.yourrights.org.uk/yourrights/privacy/article-8-the-right-to-respect-for-private-and-family-life-home-and-corresp.html>> at 16 December 2010. However, elsewhere these matters and acts violate other laws and, it has been argued, should be regulated based on: national security, the public safety, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others. Recent decision by the UN General Assembly's Third Committee on Social, Cultural and Humanitarian Issues to put to the General Assembly vote whether 'sexual orientation' should be removed from the resolution to protect people from arbitrary execution has been condemned in many parts of the world. It removal was, however, supported by Jordan, one of 79 voting in favour of the proposal - 7 against and 10 absentions.

¹⁰³ Nowak, above n 101, 89.

the provisions, aims and objectives of the ICCPR and should be, in any event, reasonable in the particular circumstances.¹⁰⁴

2.6.3 European Convention on Human Rights (ECHR (1950) Article 8)

The European Convention on Human Rights, which opened for signature in Rome on 4 November 1950, has been ratified by all Member states of the Council of Europe. The notion of the protection of privacy is expressed in Article 8 which reads:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and the freedoms of others.¹⁰⁵

The terms, with respect to privacy protection, in Article 8 of the ECHR have a broader interpretation than those in Article 17 of the ICCPR. The essential object of Article 8 is expressed in terms of protecting ‘the individual against arbitrary interference by the public authorities in his private and family life’. The right to respect for private life requires securing to the individual a sphere within which he/she can freely pursue the development and fulfillment of his/her personality.¹⁰⁶

¹⁰⁴ Edwards, above n 96, 395.

¹⁰⁵ *European Convention on Human Rights* opened for signature 4 November 1950 (entered into force 3 September 1953) art 8 <http://www.hrcr.org/docs/Eur_Convention/euroconv3.html> at 10 January 2008.

¹⁰⁶ Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6(3) *International Journal of Law and Information Technology* 247, 256.

The European Court of Human Rights, which is charged with resolving disputes arising under the ECHR, has held that Article 8 also provides some protection in regard to the ‘right to personal development, and the right to establish and develop relationships with other human beings and the outside world’,¹⁰⁷ as established in *Niemietz v Germany* in 1992, noted as stated above in *Friedl v Austria* in 1996, and clearly restated in *Pretty v United Kingdom* in 2002.¹⁰⁸

The European Court of Human Rights¹⁰⁹ has also ruled that the right to privacy of the ‘home’ extends to ‘business premises’. In *Niemietz v Germany* the Court stated that:

It would be too restrictive to limit the notion [of private life] to an inner circle in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of private life should be taken to exclude activities of a personal or business nature since it is after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of development relationship with the outside world.¹¹⁰

¹⁰⁷ *Burghartz v Switzerland* 16213/90 (1994) Eur Court HR, A280-b (22 February 1994) [2], avail <http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695742&portal=hbkmsource=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649> at 15 December 2010.

¹⁰⁸ *Niemietz v Germany* 13710/88 (1992) Eur Court HR, A251-B (16 December 1992), [29]. The quote is from para 45 of an Opinion ‘Commission’s Report’ attached as an Appendix to *Friedl v Austria* (1996) 21 EHRR 83. See also *Pretty v United Kingdom* (2002) 35 EHHR 1, [61].

¹⁰⁹ For more cases decided by the European Court of Human Rights regarding privacy, see European Court of Human Rights, ‘Key Case-Law Issues: The Concepts of Private and Family Life’ (European Court of Human Rights, 2007) <http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-DE0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf> at 15 December 2010.

¹¹⁰ See *Niemietz v Germany* 13710/88 (1992) Eur Court HR, A251-B (16 December 1992), [29], avail <www.echr.coe.int/echr/Homepage_EN> at 15 November 2008.

With respect to data protection, the European Court of Human Rights recognised the right to privacy in the context of criminal procedures, as it applied Article 8 of the European Convention.¹¹¹ In *Huvig v France*,¹¹² the Court held that ‘tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence’. Accordingly, the Court unanimously held that there had been a breach of Article 8.

Furthermore, it has been held that gender identification,¹¹³ name¹¹⁴ and sexual orientation,¹¹⁵ as well as sexual life,¹¹⁶ are caught within the meaning of Article 8. The court has given a broad meaning to privacy. Disclosure by publication of closed circuit footage of an activity in a public area was held a breach of privacy.¹¹⁷ Thus a right to privacy may extend to, or accompany a person into, a public area. Similarly the release of information, including photographs, films, and letters, to a broader audience than that intended by the person originally supplying them may be held a breach of privacy.

The right to privacy expressed in Article 17 of the ICCPR and Article 8 of the ECHR is significant for citizens in countries — like Jordan — that lack

¹¹¹ Edwards, above n 96, 397.

¹¹² See *Huvig v France* 11105/84 (1990) Eur Court HR, A176-B, (24 April 1990) [32], avail <www.echr.coe.int/echr/Homepage_EN> at 15 November 2008.

¹¹³ See *B v France* (1992) 16 EHRR 1, avail <<http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695647&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649>> at 15 December 2010.

¹¹⁴ See *Burghartz v Switzerland* (1994) 18 EHRR 101, [47].

¹¹⁵ *Dudgeon v United Kingdom* (1982) 4 EHRR 149, avail <<http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695350&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649>> at 15 December 2010.

¹¹⁶ *Dudgeon v United Kingdom* (1982) 4 EHRR 149; *ADT v United Kingdom* (2001) 31 EHRR 33.

¹¹⁷ In this instance, of the immediate aftermath of an attempted suicide, with identity of the person recognisable to those who knew him: *Peck v United Kingdom* (2003) 36 EHRR 41, [57], [60]-[61].

domestic privacy protection laws. Citizens in Jordan may be able to claim privacy protection in cases there has been violation of either or both of these articles.¹¹⁸ Growing interaction with the European Union and its member countries which must observe ECHR principles may also add some weight to domestic calls for reform. Lawmakers in Jordan may also be under a legal duty to introduce rules on privacy protection in order to comply with the ICCPR, to which Jordan is a signatory, and in relation to which it submits ICCPR periodic reports as required, the most recent being that considered in October 2010.¹¹⁹

2.6.4 American Convention on Human Rights (ACHR (1969) Article 11)

The *American Convention on Human Rights* (ACHR) was signed at the Inter-American Specialised Conference on Human Rights on 22 November 1969. The Convention entered into force on 18 July 1978. As of February 2010, it has been ratified by 25 of the 35 members of the Organisation of American States.¹²⁰ It contains provisions protecting the right to privacy that echo those recorded above. Article 11 of the Convention provides:

1. Everyone has the right to have his honor respected and his dignity recognized.

¹¹⁸ Bygrave, above n 106, 248.

¹¹⁹ Human Rights Committee, *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: Fourth Periodic Report of Jordan* (CCPR/C/JOR/4; CCPR/C/JOR/Q/4 and Add.1/HRI/CORE/1Add.18/Rev.1): 100th sess, sum record of 2748th mtg, 13 October 2010 CCPR/C/SR.2748.

¹²⁰ Namely, Argentina, Barbados, Brazil, Bolivia, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Suriname, Uruguay and Venezuela (Trinidad and Tobago having suspended their ratification in the late 1990s): Organisation of American States, Department of International Law <<http://www.oas.org/juridico/english/sigs/b-32.html>> at 27 November 2010.

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks.¹²¹

The Convention created the Inter-American Commission on Human Rights (IACHR), which has the primary goal of promoting the observance and the defence of human rights. In the case of *Ms X and Y v Argentina*,¹²² the Commission found a violation of the right to privacy, upholding complaints by Ms. X and Y (mother and daughter of a prison inmate) that while they are in prison, their right to privacy had been violated by body-cavity searches. The Commission ruled that Article 11 of the Convention protects the physical and moral integrity of the person and specifically that Article 11(2) prohibits 'arbitrary or abusive interference' with a person's private life.¹²³

2.6.5 Cairo Declaration on Human Rights in Islam (CDHR (1990) Article 18)

The *Cairo Declaration on Human Rights in Islam* (CDHR) was adopted during the Nineteenth Islamic Conference of Foreign Ministers (Session of Peace, Interdependence and Development) in Cairo (Egypt) in 1990. Article 18 of the Cairo Declaration states that:

¹²¹ *American Convention on Human Rights*, opened for signature 22 November 1969 OASTS No 36 (entered into force 18 July 1978). For text see Organisation of American States, Department of International Law <<http://www.oas.org/juridico/english/sigs/b-32.html>> at 27 November 2010.

¹²² Inter-American Commission on Human Rights, Report No 38/96, Case No 10.506, Argentina, 15 October 1996, avail <<http://www.cidh.org>> at 12 December 2008.

¹²³ Edwards, above n 96, 399.

(a) Everyone shall have the right to live in security for himself, his religion, his dependents, his honour and his property.

(b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference.

(c) A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and dwellers evicted.¹²⁴

To summarise briefly, there are no substantial differences between the Cairo Declaration and the various other conventions on human rights (further above) in regards to the privacy protection provided for individuals. The difference, however, is that the CDHR was adopted by a group of countries that share the same religion — Islam. Nevertheless the terms used in Article 18 extend privacy protection under the Declaration to ‘everyone’ not just to ‘Muslims’. Furthermore, Article 18 has prohibited specific acts such as ‘spying’ and placing individuals under ‘surveillance’, which are the most common acts that have been used by governments of the Muslim world. Nevertheless, the author believes that the CDHR (like the UDHR) is not legally binding on its signatories. Its terms are no more than set of recommendations for its members. Although privacy in Islam will be discussed in the coming chapters, it was appropriate to refer to CDHR at this stage as it is one of the supra-national conventions relevant to the subject.

¹²⁴ *Cairo Declaration on Human Rights in Islam*, adopted Nineteenth Islamic Conference of Foreign Ministers, Cairo, 5 August 1990, UN GAOR, World Conference on Human Rights, 4th sess, agenda item 5, UN Doc A/CONF.157/PC/62/Add.18 (1993) [English trans] avail <<http://www.arabhumanrights.org/publications/regional/islamic/cairo-declaration-islam-93e.pdf>> at 4 February 2010.

2.7 International Standards of Privacy

As discussed above, privacy is treated as a fundamental human right in regional and international conventions. At present, however, there is no globally agreed set of information privacy rules or standards. Instead, there are various intersecting privacy frameworks covering a number of sub-groups within the international community of states.¹²⁵ In this section, brief reference is made to the privacy protection frameworks of the Organisation for Economic Cooperation and Development (OECD) and the Asia Pacific Economic Cooperation (APEC). The frameworks of these two forums are considered because the participating countries have dominated the information technology, transborder data flows and global networks. The frameworks adopted by OECD and APEC could have significant impacts on countries – like Jordan – which do not have privacy protection laws.

2.7.1 Organisation for Economic Cooperation and Development (OECD)

The OECD Council adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (*OECD Guidelines*) on 23 September 1980, with a recommendation (which became applicable on that day) that members ‘agree as soon as possible on specific procedures of consultation and cooperation for the application of the Guidelines’.¹²⁶ The development of automatic data processing, which enables vast quantities of data to be

¹²⁵ New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 10, 165.

¹²⁶ OECD Council, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980) OECD Doc C (80) 58/Final 1 October 1980. The Member countries of the OECD are: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherland, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States.

transmitted within seconds across national borders, had made it necessary for the OECD Council to consider privacy protection guidelines in relation to personal information as such material could now flow from areas where protection existed to areas where it did not. Additionally, the OECD Council seeks to promote the free flow of personal information across borders in order to prevent any serious disruption in important sectors of the economy, such as banking and insurance.¹²⁷

The *OECD Guidelines* seek to protect ‘personal data, whether in the public or private sectors, which because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties’.¹²⁸ It sets out eight basic principles of national application for its member countries. These principles are:

1. **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

¹²⁷ Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) <<http://www.oecd.org>> at 12 December 2008. (*OECD Guidelines*). The Guidelines are an Annex to the *Recommendations of the Council of 23 September 1980: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* OECD Doc C (80) 58/Final (1 October 1980).

¹²⁸ *OECD Guidelines*, pt 1, cl 2.

4. **Use Limitation Principle:** personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle three except:
 - a) with the consent of the data subject; or
 - b) by the authority of law.
5. **Security Safeguards Principle:** personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.
6. **Openness Principle:** there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle:** An individual should have the right:
 - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
 - b) to have communicated to him, data relating to him
 - within a reasonable time;
 - at a charge, if any, that is not excessive;
 - in a reasonable manner; and
 - in a form that is readily intelligible to him
 - d) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
 - e) to challenge data relating to him and, if the challenge is successful to have data erased, rectified, completed or amended.
8. **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.¹²⁹

In addition to the above principles, the OECD Council has also adopted four basic principles to facilitate the free flow of data between members and

¹²⁹ *OECD Guidelines*, pt 2, cll 7–14.

specify circumstances that the members may impose restrictions on the transfer of data.¹³⁰ These principles are:

1. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
2. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
3. A member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
4. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.¹³¹

As Fred Cate notes:

Under the *OECD Guidelines*, data processors have certain obligations without regard for the wishes of individual data subjects. For example the data quality and security safeguards principles appear non-negotiable. Other obligations are stated more broadly and may be affected by individual consent.¹³²

The use limitation and purpose specification principles, for example, require that the use of data is restricted to the purposes for which it was collected.¹³³

The Guidelines, however, are not legally binding as they are expressed in

¹³⁰ Olujoke Akindemowo, *Information Technology Law in Australia* (1999) 235.

¹³¹ *OECD Guidelines*, pt 3, cll 15–18.

¹³² Fred H Cate, 'The Failure of Fair Information Practice Principles' in Jane K. Winn (ed), *Consumer Protection in the Age of the 'Information Economy'* (2006) 347.

¹³³ *Ibid* 347.

terms of recommendations rather than obligations.¹³⁴ The OECD recommended that member countries encourage data collectors to create codes of conduct. In response, the US Secretary of Commerce sent letters to 750 multinational corporations urging them to support the OECD Guidelines. In 1981, at an OECD follow-up meeting, the United States has reported that more than 150 corporations had given their support to the Guidelines.¹³⁵ The OECD does not have the power to enforce its recommendation, and it seems unwilling or unable to take on the contentious issue of how countries should work together to bridge their different standards of protection.¹³⁶

The breadth of the *OECD Guidelines'* purposes (including both protecting privacy and facilitating multinational data flows), and the principles and language adopted, reflect a real world flexibility and proportionality, and undoubtedly help explain their wide adoption and broad acclaim.¹³⁷ However, due to the continuing rapid development in technology, new guidelines are needed 'to embrace the outcomes of technological advances and recognise that they are overwhelmingly to the benefit of humanity'.¹³⁸ One of the main criticisms of the OECD Guidelines is the motive behind the adoption of these guidelines. The OECD is an economic forum and its main concern is an economic one: the free flow of information, and not privacy. So it is obvious

¹³⁴ Akindemowo, above n 130, 236.

¹³⁵ Pricilla M Regan, 'The Globalization of Privacy: Implications of Recent Changes in Europe' (1993) 52(3) *American Journal of Economics and Sociology* 257, 261–2.

¹³⁶ Julia M Formholz, 'Data Privacy: The European Union Data Privacy Directive' (2000) 15 *Berkeley Technological Law Journal* 461, 467.

¹³⁷ Cate, above n 132, 347.

¹³⁸ Michael Kirby, 'Privacy Protection, A New Beginning: OECD Principles 20 Years On' (1999) 6(3) *Privacy Law and Policy Reporter* 25.

that the *OECD Guidelines* seem to serve the interest of economic sectors, which need easy access to data for profitable businesses. For example, the flow of information in the banking and insurance sectors are important because they are instruments of market control, administration and organisation.¹³⁹ In summary, although the *OECD Guidelines* have brought much needed attention to the task of assuring global privacy protection, these guidelines were not based upon the view of privacy as a fundamental human right.¹⁴⁰

The above criticisms may go some way to explain the emergence of the idea of establishing regional economic cooperation between different states in different regions of the world. The best example of the regional cooperation is the Asia-Pacific Economic Cooperation which will be discussed below. Whilst the emphasis is still economic, there is a thrust to establish ‘a common set of privacy principles’.¹⁴¹

2.7.2 Asia-Pacific Economic Cooperation (APEC)

The APEC Privacy Framework,¹⁴² which was adopted on November 2004, is the most recent collection of international principles that have been adopted by the APEC members.¹⁴³ These principles have been built on the OECD

¹³⁹ Serge Gutwirth, *Privacy and the Information Age* (2002) 88.

¹⁴⁰ Julia Gladstone, 'The Impact of E-Commerce on the Laws of Nations: The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy' (2000) 7 *Willamette Journal of International Law and Dispute Resolution* 17.

¹⁴¹ APEC, 'APEC Privacy Framework' Fact Sheet (2010) <<http://www.apec.org/en/About-Us/About-APEC/Fact-Sheets/Collection/APEC-Privacy-Framework.aspx>> 27 November 2010.

¹⁴² Asia-Pacific Economic Cooperation (APEC), *APEC Privacy Framework* (2005), avail <www.apec.org> at 10 December 2008.

¹⁴³ Member countries are: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States and Viet Nam, See

guidelines, but modernised by APEC in response to the escalating demand for standards that facilitate cross-boarder flows of data.¹⁴⁴ The APEC Privacy Framework includes nine principles:

1. **Preventing Harm:** Recognising the interest of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information.
2. **Notice:** Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information.
3. **Collection Limitation:** the collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
4. **Use of Personal Information:** Personal information collected should be used only to fulfil the purposes of collection and other compatible or related purposes except: (a) with the consent of the individual whose personal information is collected; (b) when necessary to provide a service or product requested by the individual; or, (c) by the authority of law and other legal instruments, proclamations, and pronouncements of legal effects.
5. **Choice:** Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible, and affordable mechanisms to exercise choice in relation to the collection, use, and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.
6. **Integrity of Personal Information:** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
7. **Security Safeguards:** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification, or disclosure of information or

<<http://www.apec.org/en/About-Us/About-APEC/Member-Economies.aspx>> at 16 December 2010.

¹⁴⁴ Cate, above n 132, 351.

other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

8. **Access and Correction:** Individuals should be able to : (a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; (b) have communicated to them, after having provided sufficient proof of their identity, personal information about them...; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended, or deleted.
9. **Accountability:** A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.¹⁴⁵

The APEC Privacy Principles has been criticized by scholars such as Graham Greenleaf. First, Greenleaf notes that the APEC Privacy Principles are based on the OECD Principles, which have been in use for more than 20 years. The APEC Principles are only a minor improved version of those the OECD. Justice Michael Kirby, who chaired the Expert Group that drafted the OECD Principles, has stressed the need for their revision to suit the 21st Century environment.¹⁴⁶

Second: according to Greenleaf, the APEC Privacy Principles do not include the OECD Privacy Principles concerning 'Purpose Specification or Openness'

¹⁴⁵ APEC, *APEC Privacy Framework* (2005) 11–29.

¹⁴⁶ Graham Greenleaf, 'Asia-Pacific Developments in Information Privacy Law and its Interpretation' (2007) 5 <<http://www.austlii.edu.au/au/special/privacy/>> at 6 March 2009.

and are therefore, weaker on those counts. In addition, he notes that the new principles of ‘preventing harm’ and ‘choice’ carry inherent dangers and have little to recommend them.¹⁴⁷

Finally: the APEC Privacy Framework fails to embrace other regional privacy principles that are stronger than those found in the *OECD Guidelines*, which means that the APEC Framework does not take into consideration the experiences of those Asia-Pacific countries that do have privacy laws. National privacy laws for some Asia-Pacific countries go beyond privacy principles of the OECD. The use of APEC Privacy Framework ignores the opportunity to share these national privacy laws across multiple Asia-Pacific jurisdictions. The APEC Principles, therefore, do not represent any objective ‘consensus’ among existing regional privacy laws, unless on the basis of the lowest common denominator of every privacy principles legislation in the region.¹⁴⁸

In sum, however, while it is valuable to consider the various international instruments and their approaches to privacy protection, it should be noted that, with the exception of the *Cairo Declaration on Human Rights in Islam* (1990) to which it has agreed and the *Arab Charter of Human Rights* (as amended) 2004 to which it has acceded (and both of which are guiding documents rather than treaties with obligations attached),¹⁴⁹ Jordan is not a signatory to any of the regional instruments listed above (geography

¹⁴⁷ Ibid.

¹⁴⁸ Ibid.

¹⁴⁹ Arab Human Rights Index, *Jordan*
<<http://www.arabhumanrights.org/en/countries/country.aspx?cid=7>>.

necessarily excluding it from a number of them).¹⁵⁰ Therefore, the regional instruments are not legally binding on Jordan. Furthermore, these instruments and their respective bodies established by them do not play a supervisory role in how Jordan can process (collect, access, transfer) personal information. In terms of the privacy principles they contain, however, they have a recommendatory rather than an enforcement role in the creation of domestic privacy principles in Jordan and their implementations. As has been noted above, both the *Cairo Declaration on Human Rights* and the amended *Arab Charter of Arab Human Rights* offer guidance to their signatories rather than imposing binding obligations. Jordan is, however, a signatory to the ICCPR.¹⁵¹

2.8 Concluding Remarks

This Chapter has presented an overview of some of the definitions of the concept of ‘privacy’. The lesson here is that ‘privacy’ is an ill-defined but nevertheless well-understood concept. It is ill-defined because people use the term in many different ways that reveal the various meanings attributed to it. The literature review on privacy has revealed that privacy is a complicated concept that remains difficult to define. One simple reason for this complexity is that the definition of privacy differs from one culture to another. For example, in some cultures (like that of Jordan), concepts such as honour and reputation are strong elements of a person’s privacy. These are strong values and seen as the collective property of the family and thus when

¹⁵⁰ ECHR, ACHR, *OECD Guidelines*, APEC.

¹⁵¹ Since 1975. See UNHCHR treaties database, above n 97.

the honour of a person is impugned, the honour of all is perceived as affected.¹⁵² As a result, people in such culture, will defend the honour of their families without regard for culpability.¹⁵³ However, in western cultures, defending these concepts (honour and reputation) does not reach the same level as that of Jordan.

The value of privacy in some cultures is a very important one for which to legislate and to protect as a human right. It also has implications in regard to other rights. In Jordan, for example, cultural values such as honour, reputation, democracy and freedom of speech are influenced by the extent to which privacy is preserved and protected. The author believes that the recognition and protection of the right to privacy is significant for Jordan if the country is to achieve its objectives of promoting the democracy, protecting freedom of expression, maintaining transparency, and fighting against corruption and crime. In order to maintain these values, privacy should be explicitly considered as a fundamental human right rather than property right.

Finally, Jordanians could bid for the right to privacy, encouraged by the moral suasion of the UDHR and the CDHR, and the model offered by the ECHR, or attempt to legally claim the right of privacy in accordance with the ICCPR. All of these documents (unlike the OECD and APEC documents)

¹⁵² And indeed both reputation and future prospects of all members can be adversely affected, which in a number of cases has prompted violent action by family members against the family member deemed to have brought shame on the family: see, Hanna Cinthio and Marcus Ericsson, 'Beneath the Surface of Honour: A Study on the Interplay of Islam and Tribal Patriarchy in Relation to Crimes of honour in Jordan' (Lund University, 2006) 21-4, 33-4, 36, 50-1.

¹⁵³ Norhayati Zakaria, Jeffrey M Stanton and Shreya TM Sarkar-Barney, 'Designing and Implementing Culturally-sensitive IT Applications: The Interaction of Culture Values and Privacy Issues in the Middle East' (2003) 16(1) *Information Technology and People* 49, 64.

have emphasised the right to privacy as a fundamental human right. This condition of privacy has also been emphasised by the *Shari'ah* which is the root of the Jordanian legal system. The next chapter illustrates the many occasions where this fundamental human right is well recognised and protected in Islam.

Chapter Three

Privacy in Islam

3.1 Introduction

In the previous chapter, the concept of privacy has been broadly explained from the point of view of western literature. This chapter continues to explore the concept of privacy from another and more specific point of view; the right to privacy in Islam. There are several reasons for the discussion of privacy in the Islamic context. First, the Jordanian legal system is based on the Civil Law which is, in turn, founded on the principles of *Shari'ah* (Islamic Law). Laws and regulations in Jordan generally stem from the *Shari'ah*. Therefore, it is appropriate to understand the position of Islam towards privacy. Second, Jordan is a predominantly Muslim country, so Islamic values and principles play an important role in the lives of the Jordanian people. Privacy as a concept in Islam is protected and maintained on many occasions within Islam itself; however, this concept is not clearly understood within a legal framework in the context of Jordan. Finally, and most importantly, the *Shari'ah* considers privacy as a fundamental human right. This right is supported in many passages in two of the main sources of *Shari'ah*: The *Holy Qur'an* and *Sunnah*. These sources provide significant legal foundations that constituted a right to privacy long before the international documents on human rights discussed in the above chapter did so.

There are other sources of the *Shari'ah* that recognise the right to privacy, including Ijma (consensus of opinion), *Qiyas* (analogical deduction) and *Ijtihad* (personal reasoning). In respect to the right of privacy this chapter is only focusing on the main primary sources of *Shari'ah*: the *Holy Qur'an* and *Sunnah*. There are many passages in the *Qur'an* and *Sunnah* that address aspects of the right to privacy. These aspects are: (1) privacy of the home, (2) suspicion and espionage, (3) private correspondence, (4) confidential conversation, (5) privacy of non-Muslims, and (6) privacy of the deceased persons. Further, this chapter intends to explore the role of government in protecting privacy in accordance with the *Shari'ah*. However, this chapter begins by briefly defining the sources of the Islamic law.

3.2 The Sources of the *Shari'ah* (Islamic Law)

3.2.1 The *Holy Qur'an*

The *Qur'an*, which Muslims believe to be the literal and final word of God, was collected very early in Muslim history. The text of the *Qur'an* is accepted as accurate and beyond dispute by all Muslims.² The *Qur'an* contains clear and unambiguous instructions in details on matters relating personal status (marriage, divorce, inheritance) and to particular transgressions of the law. It is generally held that the *Qur'an* contains no more than 500 verses³ concerning legal matters, of which 80 are legislative in the strict sense of the

¹ Note, unless otherwise stated, all quotations from the *Holy Qur'an* are from: *The NOBLE QUR'AN: Translation of the Meanings of the Noble Qur'an in the English Language: by Dr Muhammad Taqi-ud-Din al-Hilali and Dr Muhammad Muhsin Khan* (King Fahd Complex for the Printing of the HOLY QUR'AN).

² Abdullahi Ahmed An-Na'im, *Toward an Islamic Reformation: Civil Liberties, Human Rights, and International Law* (1990) 19.

³ This is of the over 6300 verses that form the *Qur'an*.

term.⁴ The remainder contains the basic notions underlying civilised society, such as: compassion, fairness and good faith in commercial transactions and integrity and incorruptibility in the administration of justice, and expresses them as the Islamic principles for human rights.⁵ Some Muslim scholars conclude that there are five human rights principles under Islamic law: (1) dignity and brotherhood; (2) equality among members of the community, without discrimination on the basis of race, colour or class; (3) respect for the honour, reputation and family of everyone; (4) the presumption of innocence; and (5) individual freedom.⁶

The above principles appear in many verses of the *Qur'an*. Principally, the *Qur'an* places an infinite value upon human life. Expressing this principle, the *Qur'an* says:

مَنْ أَجَلِ ذَلِكَ كَتَبْنَا عَلَىٰ بَنِي إِسْرَائِيلَ أَنَّهُ مَنْ قَتَلَ نَفْسًا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِي الْأَرْضِ
فَكَأَنَّمَا قَتَلَ النَّاسَ جَمِيعًا وَمَنْ أَحْيَاهَا فَكَأَنَّمَا أَحْيَا النَّاسَ جَمِيعًا ۚ وَلَقَدْ جَاءَتْهُمْ رُسُلُنَا
بِالْبَيِّنَاتِ ثُمَّ إِن كَثِيرًا مِّنْهُمْ بَعَدَ ذَلِكَ فِي الْأَرْضِ لَمُسْرِفُونَ ﴿١٥١﴾

⁴ Patrick Bannerman, *Islam in Perspective: A Guide to Islamic Society, Politics and Law* (1988) 34.

⁵ An-Na'im, above n 2, 20.

⁶ Kamran Hashemi, *Religious Legal Traditions, International Human Rights Law and Muslim States* (2008) 11.

In translation: ⁷

...That if any one slew a person — unless it be for murder or for spreading mischief in the land — it would be as if he slew the whole people: and if any one saved a life, it would be as if he saved the life of the whole people...

According to the Qur'an, God's love, grace and providence are universal, embracing all human beings as the sunlight. God states:⁸

﴿ وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ وَالْبَحْرِ وَرَزَقْنَاهُمْ مِنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ مِمَّنْ خَلَقْنَا تَفْضِيلًا ﴾

And indeed we have honoured the Children of Adam, and we have carried them on land and sea, and have provided them with At-Taiyibât (Lawful good things), and have preferred them above many of those whom we have created with a marked preference.

Therefore, all human beings have honour, inviolability and dignity. Human beings should treat each other with dignity — the way God treats them.⁹ The dignity of the human life is intrinsic to someone's personality and no regime, however powerful, should take it away. Such dignity could be offended by ridicule, defamation and sarcasm. Mutual ridicule, arrogance and selfishness are not amusing.¹⁰ As God states:

⁷ Surat No 5 - Al-Maidah, Section 6, Aya 32, *The Holy Qur'an*, 293.

⁸ Surat No 17 - Al-Israa, Section 15, Aya 70, *The Holy Qur'an*, 799.

⁹ Recep Senturk, 'Sociology of Rights' in Abdul Aziz Said, Mohammed Abu-Nimer and Meena Sharify-Funk (eds), *Contemporary Islam: Dynamic, not Static* (2006) 36.

¹⁰ Sayed Khatab and Gary D Bouma, *Democracy in Islam* (2007) 103.

يَتَأْتِيهَا الَّذِينَ ءَامَنُوا لَا يَسْخَرُونَ قَوْمًا مِّن قَوْمٍ عَسَىٰ أَن يَكُونُوا خَيْرًا مِّنْهُمْ وَلَا نِسَاءً مِّن نِّسَاءٍ عَسَىٰ أَن يَكُنَّ خَيْرًا مِّنْهُنَّ وَلَا تَلْمِزُوا أَنفُسَكُمْ وَلَا تَنَابَزُوا بِاللِّقَابِ بئْسَ الْإِسْمُ الْفُسُوقُ بَعْدَ الْإِيمَانِ ۚ وَمَن لَّمْ يَتُبْ فَأُولَٰئِكَ هُمُ الظَّالِمُونَ ﴿٥١﴾

The translation of this verse is as follows:

O ye who believe! Let not some men among you laugh at others. It may be that the latter are better than the former: nor let some women laugh at others: it may be that the latter are better than the former: nor defame nor be sarcastic to each other,¹¹

3.2.2 The *Sunnah*

The second most important source of Islamic law is the *Sunnah*. The literal meaning of the Arabic word *Sunnah* is ‘habit, practice, customary procedure, action, norm and usage sanctioned by tradition’.¹² However, the term *Sunnah* in the Islamic legal system means all the acts and sayings of the Prophet Muhammad (*Peace be upon Him (pbuh)*), as well as everything he approved. Only *Sunnah* of a legal nature is held to form part of the *Shari’ah*. Personal practices of the Prophet, such as the way he dressed and ate, and sayings relating to such matters as agriculture and the strategy of the wars fought at the time, are not considered as forming part of the *Shari’ah*.¹³

Muslim jurists use the *Sunnah* for the following purposes in determining the law:

¹¹ Surat No 49 – *Al-Hujurat*, Section 26, Aya 11, *The Holy Qur’an*, 1591.

¹² Zafar Iqbal and Mervyn K Lewis, *An Islamic Perspective on Governance* (2009) 30.

¹³ Jamila Hussain, *Islam: Its Law and Society* (second ed, 2004) 32.

- (1) To confirm the law that has already been mentioned in the Qur'an;
- (2) To give an adequate explanation to matters which have been mentioned in the Qur'an in general terms only;
- (3) To clarify verses in the Qur'an where there may be some ambiguity;
- (4) To introduce a new rule which is not mentioned in the Qur'an, for example, the prohibition on marrying an aunt and niece at the same time.¹⁴

Thus, the difference between the two sources, the *Holy Qur'an* and the *Sunnah*, is that the first source contains general principles of social order while the second demonstrates the application of these principles in the peoples' way of life, as a community and a state, all under the auspices of the Prophet Muhammad (pbuh).¹⁵ The *Sunnah* is extracted from the reports called *Hadith* (plural: *Ahadith*) that record the Prophet's sayings, actions, and acts approved by him.¹⁶

3.3 *Shari'ah* and Some Aspects of Privacy

3.3.1 Privacy of the Home

The *Qur'an* and *Sunnah* establish major rules to protect individual privacy when people are at home. It can be said that the *Qur'an* has clearly constituted the right to privacy in the home. This appears in the following verses:

يَأْتِيهَا الَّذِينَ ءَامَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ

خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ ﴿١٦﴾

¹⁴ Ibid.

¹⁵ Iqbal and Lewis, above n 12, 30.

¹⁶ Ibid 31.

O ye who believe! Enter not houses other than your own, until ye have asked permission and saluted those in them: that is best for you, in order that ye may heed (what is seemly).¹⁷

In another explicit verse:

فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ^ط وَإِنْ قِيلَ لَكُمْ ارجِعُوا

فَارْجِعُوا^ط هُوَ أَزْكَى لَكُمْ^ع وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ ﴿٢٨﴾

If ye find no one in the house, enter not until permission is given to you: if ye are asked to go back, go back: that makes for greater purity for yourselves: and Allah knows well that ye do.¹⁸

The above verses stipulate clear commandment to not enter the house of others unless consent is manifestly given. The logic behind this is obvious: if one does not receive any permission to enter, it means the people in the house do not want intrusion at that time. One has no right to enter someone's house without permission, even if no one is inside.¹⁹ The above verses are in general terms, which means that they are applicable to everyone, including one's relatives, men, women, and even children, government authorities and the police, without exception.²⁰

Furthermore, the Qur'an prohibits entering premises secretly or through back doors. It requires persons to identify themselves to the residents and to

¹⁷ Surat No 24 – An-nur, Section 18, Aya 27, The Holy Qur'an, 1011.

¹⁸ Surat No 24 – An-Nur, Section 18, Aya 28, The Holy Qur'an, 1011.

¹⁹ Muhammad Aslam Hayat, 'Privacy and Islam: From the Quran to Data Protection in Pakistan' (2007) 16(2) *Information and Communications Technology Law* 137, 138.

²⁰ Mohammad Hashim Kamali, *The Right to Life, Security, Privacy and Ownership in Islam* (2008) 166.

enter premises through front doors.²¹ The following verse of the Qur'an, gives instructions and guidance on how to enter premises:

﴿ يَسْأَلُونَكَ عَنِ الْأَهْلِ قُلْ هِيَ مَوَاقِيتُ لِلنَّاسِ وَالْحَجِّ ۗ وَلَيْسَ الْبِرُّ بِأَنْ تَأْتُوا الْبُيُوتَ مِنْ ظُهُورِهَا وَلَكِنَّ الْبِرَّ مَنِ اتَّقَى ۗ وَأْتُوا الْبُيُوتَ مِنْ أَبْوَابِهَا ۚ وَاتَّقُوا اللَّهَ لَعَلَّكُمْ تُفْلِحُونَ ﴾

They ask thee concerning the New Moons. Say: they are but signs to mark fixed periods of time in (the affairs of) men, and for Pilgrimage. It is no virtue if ye enter your houses from the back: it is virtue if ye fear Allah. Enter houses through the proper doors. And fear Allah: that ye may prosper.²²

The *Sunnah* also established many rules in order to protect an individual's privacy at home. It has reported that the Prophet went to the extent of instructing that a man should not enter his own house suddenly; he should indicate to the dwellers of the house that he is coming.²³ The following *Hadith* is an explanation of the Qur'anic verse on the subject of seeking permission before entry:

It has reported that a man asked the Prophet: 'O Messenger of God, do I (need to ask my mother for permission?)' to this the Prophet replied 'Yes'. Then the man said: 'I live with her in the house'. To this the Messenger of God responded 'Ask her permission when you enter'. The man further added 'I serve her'. Then the Prophet said 'seek her permission. Do you wish to see her naked?' The man said 'No'. To this, the reply came 'then ask her for permission'.²⁴

However, while most Muslim scholars — if not all — recognise the principle of the sanctity of the home, they have disagreed on the question of the legal

²¹ Hayat, above n 19, 138.

²² *Surat No 2 – Al-Baqarah, Section 1, Aya 189, The Holy Qur'an*, 79.

²³ Sheikh Showkat Husain, 'Human Rights in Islam Principles and Precedents' in Tahir Mahmood (ed), *Human Rights in Islamic Law* (1993) 88.

²⁴ Al-Bukhari, 'Kitab al adab al mufrad' Hadith No (1059) & No (1060) [Arabic].

basis of this principle: that is, is the sanctity of the home based on the right to privacy or on the right to property?

One view is that the sanctity of homes is based on the right to property. This view claims that unoccupied homes cannot be entered unless: (1) there is property that belongs to the person who is trying to obtain it by entering the home; and (2) this home is unoccupied. Therefore, the right to obtain someone's own property takes precedence over the right of the homeowner who has the right to refuse the person's entry without supplying any proper reason.²⁵ This view is based on the *Qur'anic* verse which says:

لَيْسَ عَلَيْكُمْ جُنَاحٌ أَنْ تَدْخُلُوا بُيُوتًا غَيْرَ مَسْكُونَةٍ فِيهَا مَتَاعٌ لَكُمْ ۗ وَاللَّهُ يَعْلَمُ مَا تُبْدُونَ وَمَا تَكْتُمُونَ ﴿١١٠﴾

It is no fault on your part to enter houses not used for living in, which serve some other use for you: and Allah has knowledge of what you reveal and what you conceal.²⁶

The other view states that the sanctity of homes exists to protect the private affairs of individuals' lives. There is no connection between this sanctity and the right to property. For instance, a tenant of the house enjoys the same security as the owner of this house under such a view. In addition, this sanctity of the home is provided to protect the right of privacy of the occupants rather than their property. This view explains that the right to someone's privacy may be violated in his/her house at the same time as there is no violation of the right of property. For example, someone's listening

²⁵ Emad Hamdy Hijazi, *Al haq fel Khosoya wa Masooliyat Al sahafy: Fe Doo2 Ahkam Alsharee'a Aleslamiya wal Alganoon Almadany* (2008) 111.

²⁶ *Surat No 24 – An-Nur, Section 18, Aya 29, The Holy Qur'an*, 1011.

through the door violates the right to privacy of others without violating their right to property.²⁷

The author favours this second view where the sanctity of the home is to protect the personal lives of individuals rather than their property. Most of the activities occurring in homes cannot be obtained in a tangible form without compromising a person's domestic privacy (for example, with the use of recording devices focused on but not actually present on the site). Personal conversations or gestures of intimate relationships (kissing, hugging, and so forth) can only be preserved when the right to privacy, not the right to property, is respected.

3.3.2 Suspicion and Espionage

It has said above that human dignity which requires the respect for honour, reputation and family matters is one of the basic principles of Islamic human rights. The *Qur'an* warns repeatedly against persecution, denounces aggression, warns against violations of this principle and reminds believers of the need to observe justice in all their dealings.²⁸ For instance, the *Qur'an* demands people to avoid all types of suspicion for it does cruel injustice to innocent individuals and groups.²⁹ As one verse of the *Qur'an* asserts:

²⁷ Hijazi, above n 25, 111.

²⁸ C G Weeramantry, 'Islam and Human Rights' in Tahir Mahmood (ed), *Human Rights in Islamic Law* (1993) 15.

²⁹ Khatab and Bouma, above n 10, 103.

يَتَأَيُّهَا الَّذِينَ ءَامَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم
بَعْضًا ؕ اُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ؕ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ



O ye who believe! *Avoid suspicion* as much (as possible): for suspicion in some cases is a sin: and *spy not on each other, nor speak ill of each other* behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it ... but fear Allah: for Allah is Oft-Returning, most Merciful.³⁰

Or as one translator explains and expands the text,

No one would even like to think of such an abomination as eating the flesh of his brother. But when the brother is dead, and the flesh is carrion, abomination is added to abomination. In the same way, people are asked to refrain from hurting people's feelings when they present: how much worse it is when say things, true or false, when they are absent.³¹

The *Sunnah* is equally emphatic on the subject of unfounded suspicion, which is seen to be the starting point of defamation and even espionage.³² The Prophet has explicitly warned people to:

[b]eware of suspicion, for suspicion is the worst of false tales. And do not count others' faults, *do not spy*, do not be envious of one another, do not desert (cut your relation with) another, and do not hate one another. And be brothers (as Allah has ordered you).³³

In regard to speaking ill of one another, the Prophet further expands the definition when he includes both true and untrue statements about another,

³⁰ Surat No 49 – *Al-Hujurat*, Section 26, Aya 12, *The Holy Qur'an*, 1593 (emphasis added). This verse emphasises that the evil of damaging a person by what we say when they are in our company is not lessened by their absence or death, rather it is made worse.

³¹ *The Meaning of the Holy Qur'an: Translated by Abdullah Yusuf Ali, Secretariat for Asia Assembly of Ulama* (2005) 395 n 534.

³² Kamali, above n 20, 197.

³³ *The Translation of the Meanings of Summarized Sahih Muslim: Arabic-English, Vol 2, Compiled by Al-Hafiz Zakiuddin Abdul-Aziz Al-Mundhiri, Published by Darussalam, Riyadh, Saudi Arabia* (2000) (*Sahih Muslim*) ch 41, 959, see Sahih Al-bukhari, Hadith 6064 (emphasis added).

distinguishing 'backbiting' from 'slander' (and thus defamation). For the prophet said, when asked what if the person who speaks poorly of another finds the failing of the brother actually exists, the Hadith says:

Backbiting is talking about your brother in a manner which he does not like. It was said to him: if what I say about him is true? He said: if what you say is true, then you backbite him, and if it is not, then you slander him.³⁴

While the distinction is made between idle gossip and baseless rumour (slander), both that and talking ill of another where in fact there appears to exist some guilt, the damage done by both to the party concerned is recognised.

In regards to espionage, the *Qur'anic* verse (cited at the beginning of this subsection) by prohibiting the act of espionage³⁵ constitutes the right to respect for personal life. Individuals must not spy on each others, or spread gossip and rumours about each other nor remain present to hear or receive to such material. The legal implication in this context is the prohibition of the solicitation, collection and dissemination of information about a person by unlawful means.³⁶

Further, reports from *Ahadith* indicate that peeping through door cracks and eavesdropping from behind closed doors were a cause for concern during the Prophet's time, and provoked a rigorous response from him.³⁷ The Prophet

³⁴ Ibid ch 44, 960.

³⁵ *Surat No 49 – Al-Hujurat, Section 26, Aya 12, The Holy Qur'an*, 1593.

³⁶ Ida Madieha Azmi, 'Personal Data Protection Law: The Malaysian Experience' (2007) 16(2) *Information and Communications Technology Law* 125, 132.

³⁷ Kamali, above n 20, 185.

states that if a man upon finding another man peering secretly into his house, blinds the latter, this action would make the former liable for prosecution.³⁸

It has narrated that:

A man peeped through a hole in the door of the Messenger's house, and at that time, the Messenger of Allah (pbuh) had a Midri (an iron comb or bar) with which he was rubbing his head. So, when the Messenger of Allah saw him, he said to him, 'if I had been sure that you were looking at me (through the door), I would have poked your eye with this (sharp iron) bar.' The Messenger added, 'Asking for permission to enter has been enjoined so that one may not look unlawfully (at what inside the house).'³⁹

With respect to person's liability, for instance, the Prophet (pbuh) states in another Hadith:

A man peeped into a room of the Prophet, peace be upon him. The Prophet stood up, holding an arrowhead. It is as if I am just looking at him, trying to stab the man.⁴⁰

The lesson from the above is that the Prophet wanted to attack the eye of the intruder without warning him. Although the attempt was unsuccessful and the man disappeared, the incident has been taken to imply that the prophet had actually meant to do it. Muslim scholars have concluded that the victim of a similar attempt is entitled to act similarly in order to defend his right to privacy, and if he strikes the intruder with a sharp instruments, a stick or stone which injures or kills him, there no liability for compensation.⁴¹

³⁸ Husain, above n 23, 88.

³⁹ *Sahih Muslim*, above n 33, ch 25, 756. See Sahih Al-Bukhari, Hadith 6901.

⁴⁰ Ibid ch 26, 756. See Sahih Al-Bukhari, Hadith 6887.

⁴¹ Kamali, above n 20, 186.

From the above *Ahadith*, the author believes that people should not be questioned and judged on the basis of baseless and weak information or doubts. Such judgments may cause harm not just for individuals the subject of the communications, but also to family members and the whole society. In Islam, human relationships are, fundamentally, based on purity, transparency and mutual respect rather than on suspicion and speculation. Therefore, the *Shari'ah* prohibits the dissemination of any kind of information about others in order to protect the principle of the sanctity of the human dignity.

Despite above *Ahadith* were directed at 'Muslims', it can be said that these rulings and instructions given by the Prophet (pbuh) apply to non-Muslims at the same level (see 3.4 further below).

This principle is reflected in the following verses of the *Holy Qur'an*, which says:

وَمَا أَرْسَلْنَاكَ إِلَّا كَافَّةً لِّلنَّاسِ بَشِيرًا وَنَذِيرًا وَلَٰكِنَّ أَكْثَرَ النَّاسِ لَا يَعْلَمُونَ



We have not sent thee But as a Messenger to all mankind, giving them Glad tidings, and warning them (Against sin), but most men know not.⁴²

3.3.3 Private Correspondence

Opening other people's personal letters and confidential correspondence falls under the *Qur'anic* prohibition of espionage.⁴³ The subject has also been

⁴² *Surat No 34 –Saba, Section 22, Aya 28, The Holy Qur'an*, 1284.

⁴³ Kamali, above n 20, 193.

specifically addressed in the *Sunnah* in which the Prophet is reported to have said:

Do not cover the walls. he who sees the letter of his brother without his permission, sees Hell-fire.⁴⁴

Unauthorised peeping into other people's letters and personal correspondence is tantamount to espionage. Letters and messages sent by post, email, fax and text messages are regarded as deposits (*wadia*) on behalf of their senders and the persons to whom they are addressed. The sender (depositor) is entitled to his rights of privacy and ownership, and these must be respected by post office employees and others. The recipient also cannot divulge confidential information that the sender has addressed only to him. This applies to all correspondence, packets and parcels.⁴⁵

3.3.4 Confidential Conversation

The *Qur'an* and *Sunnah* inculcate the ethics of trustworthiness (*amana*) most comprehensively, and discourage the betrayal of trust (*khiyana*) so strongly that *amana* becomes a central feature of the ethos Islam. Therefore, in regards to a conversation between two persons in confidence, this conversation should not be revealed to others.⁴⁶ In this context, the *Qur'an* states:

يٰۤاَيُّهَا الَّذِيْنَ ءَامَنُوْا لَا تَخُوْنُوْا اللّٰهَ وَالرَّسُوْلَ وَخُوْنُوْا اٰمَنَتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ ﴿٢٤٠﴾

⁴⁴ Sunan Abu Dawud, (Kitab Al-Salat) Bk 8, Hadith 1480, translated by Ahmad Hasan, avail http://www.searchtruth.com/hadith_books.php#abudawud at 19 December 2010.

⁴⁵ Kamali, above n 20, 193.

⁴⁶ Ibid 211.

O ye that believe! Betray not the trust of Allah and the Messenger, nor misappropriate knowingly things entrusted to you.⁴⁷

The evidence of the *Sunnah* is emphatic on the question of honouring a trust, to the point that disregarding it is equated with a flaw in the integrity of one's faith.⁴⁸ It has declared in one *Hadith* that:

The one who has no trust (*amana*) has no faith.⁴⁹

The significance of this *Hadith* amounts to a prohibition of exposure or betrayal of what has been said to one in confidence, especially if this betrayal is likely to be harmful to one's friend and confidant.⁵⁰

It is also forbidden to disclose the private affairs between husband and wife. The *Shari'ah* has demanded such information be private, especially when it comes to the intimate information. It has considered such disclosure to be one of the most sinful acts due to severe damages that one party may suffer.⁵¹

The *Hadith* of the Prophet says:

The most evil of the people to Allah on the Day of Resurrection will be the man who consorts with his wife and then publicises her secret"⁵²

Furthermore, it is prohibited to disclose the confidential information that is conveyed during a consultation or in a meeting, whether of two or more persons, which is held in an atmosphere of trust.⁵³ The *Hadith* says:

⁴⁷ Surat No 8 – *Al-Anfal*, Section 3, Aya 27, *The Holy Qur'an*, 476.

⁴⁸ Kamali, above n 20, 212.

⁴⁹ Ahmad Ibn Hanbal, *Musnad*, Vol III, 135.

⁵⁰ Kamali, above n 20, 212.

⁵¹ Hijazi, above n 25, 131.

⁵² *Commentary on the Riyad-us-Saliheen*, Compiled by Al Imam Abu Zakariya Yahya bin Sharaf An-Nawawwi Ad-Dimashqi, Vol 1, (Darussalam, 1999), Riyadh-Saudi Arabia. (1999) ch 85, 583.

⁵³ Kamali, above n 20, 213.

The participants of a council are bearers of a trust (*amana*), and it is not permissible for any one of them to reveal what the others would dislike to be exposed.⁵⁴

Another Hadith on the same subject notes:

It is not permissible for anyone to enter a meeting wherein people are engaged in consultation.⁵⁵

Consultation, however, extends to community affairs as well as to personal relations between individuals. The one who gives or receives counsel is bound to be entrusted with confidential information of one kind or another.

The one whose counsel is solicited is the bearer of trust (*amana*).⁵⁶

The ruling of the above *Hadith* may be extended by analogy to consultant physicians, family doctors and lawyers, who are usually entrusted with confidential information by their clients.⁵⁷ It is worth noting that the above *Hadith* provides a precise definition of the term of ‘confidentiality’ as discussed in the previous chapter. This appears in the current codes and policies for many businesses in Jordan where confidentiality is mainly based to a great extent on the above *Hadith*.

The issue addressed by the current research is whether the above rulings can be extended to new aspects of privacy that have accompanied the explosion of ICTs. The author believes that *Shari’ah* principles are expandable and *Shari’ah* has the ability to address and contain privacy issues that may arise

⁵⁴ Abu Dawud, ‘Awm al-Ma’bud, vol XIII, 217 [Arabic].

⁵⁵ Al-San’ani, Subul al-Salam, vol. IV, 119 [Arabic].

⁵⁶ Abu Dawud, Mukhtasar Sunan Abi Dawud, Ketab al-Adab, b. fi’l-mashwara, Hadith 5128 [Arabic].

⁵⁷ Kamali, above n 20, 216.

from the use of the new technologies. For instance, divorcing someone’s wife via sending a text message (SMS) will be considered by the family court (governed by *Shari’ah*), as an effective action and this will create its own implications. Regarding individual privacy, digital divorcing plays a crucial role in husband-wife relationship. As part of this relationship, there is a legal and moral obligation not to disclose confidential information to a third party. For example, when a husband sends a divorce notification to his wife, copying this message to his lawyer to act on it, it is believed that this private communication between husband and wife has been compromised by the lawyer (third party).

3.4 The Privacy of Non-Muslims

It is Muslim belief that the Prophet Mohammad (pbuh) was sent by God to all humankind. His principles, guidance, advice, and instructions on terms such as human dignity, honour and freedom are global, that is to say the directives are equally applicable to Muslims and non-Muslims, with no distinction between them. The Qur’an says:

قُلْ يَتَأْتِيهَا النَّاسُ إِنِّي رَسُولُ اللَّهِ إِلَيْكُمْ جَمِيعًا الَّذِي لَهُ مُلْكُ السَّمَوَاتِ وَالْأَرْضِ لَا إِلَهَ إِلَّا هُوَ يُحْيِي وَيُمِيتُ فَآمِنُوا بِاللَّهِ وَرَسُولِهِ النَّبِيِّ الْأُمِّيِّ الَّذِي يُؤْمِنُ بِاللَّهِ وَكَلِمَاتِهِ وَاتَّبِعُوهُ لَعَلَّكُمْ تَهْتَدُونَ ﴿١٥٨﴾

Say: “O men! *I am sent unto you all, as the Messenger of Allah, to Whom belongs the dominions of the heavens and the earth: there is no god but He: it is He that gives both life and death. So believe in Allah and his Messenger, the*

unlettered Prophet, who believes in *Allah* and His Words: follow him that ye may be guided.”⁵⁸

This Qur’anic verse is directed to all people not just Muslims. Muslims and non-Muslims are treated equally in regard the protection of their privacy. Although the above discussions are mainly directed to the believers (Muslims), there is no evidence that the above verses of the *Qur’an* and *Ahadith* do not apply to the non-Muslims. Non-Muslims in any Muslim society enjoy the right to privacy at home, in their private relationships, their correspondence and confidential conversations as much as Muslims. This supported in the below verse of the *Qur’an* when speaks of the dignity of humankind. The *Qur’an* says:

﴿ وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْوَجْرِ وَالْبَحْرِ وَرَزَقْنَاهُمْ مِنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ

مِمَّنْ خَلَقْنَا تَفْضِيلًا ﴾

We have honoured the sons of Adam; provided them with transport on land and sea; given them for sustenance things good and pure; and conferred on them special favours, above a great part of our creation.⁵⁹

The reference to the dignity of man in this verse is substantiated by the rank he is given over most of God’s creatures, as well as by the affirmation of his freedom of movement to traverse the land and the sea.⁶⁰ This reference is directed to all people with no-one person or group favoured above another.

3.5 The Privacy of the Deceased Persons

⁵⁸ Surat No 7 – *Al-A’raf*, Section 9, Aya 158, *The Holy Qur’an*, 451 (emphasis added).

⁵⁹ Surat No 17 – *Al-Israa*, Section 15, Aya 70, *The Holy Qur’an*, 799.

⁶⁰ Kamali, above n 20, 75.

The *Shari'ah* has demanded that people should refrain from exposing the weaknesses of the deceased persons. The dignity of the person alive does not expire at his/her death. Thus the *Sunnah* demands believers:

Mention your deceased persons for their virtues, and restrain yourselves from discussing their failings.⁶¹

However, a number of Islamic scholars have different views on whether the right to privacy of a deceased person can be transferred to his/her relatives after the death. One view is that the right to privacy cannot be transferred to others upon the death of the person. The relatives of the dead person cannot claim this right for themselves. However, they have the right to protect the dignity and honour of their dead relative if their dignity and honour would be damaged by the publication of his/her private affairs. However, this is not to say that their defence is based on the privacy right of their deceased person, but rather is based on their own right to privacy.⁶²

The second view sees the right of privacy of a dead person is a right which can be transferred to relatives after his/her death. This viewpoint is supported by arguments that state that some rights (such as, author's rights and the rights of reputation) are similar to the right of privacy and these rights are transferrable to the dead persons' relatives. Moreover, these rights constitute the moral identity of the person which in turn must be protected after the death. For example, relatives can file a law suit against anyone who

⁶¹ Sunan Abu Dawud, (Kitab Al-Adab) Bk 41, Hadith 4882, translated by Ahmad Hasan, avail <http://www.searchtruth.com/hadith_books.php#abudawud> at 19 December 2010.

⁶² Hijazi, above n 25, 219.

infringes an author's copyright.⁶³ Similarly, the right to privacy of the deceased person can be protected and defended by relatives if it is seen to touch upon their own honour or reputation.

This research favours the second view on this matter. The right of privacy is a part that is attached to the human identity. If a person has the right to protect his/her reputation and honour when he/she is alive, there is also a need to protect this reputation and this honour after the death. For example, the attack on the character of the Prophet Mohammad (pbuh) by a Danish cartoon did not cause damage to the Prophet's relatives but it did cause moral damage to millions of Muslims around the world. The sustained moral damages, here, touched the core identity of Muslims rather than the Prophet Mohammad himself. Muslims — in the author's view — are here seen as the recipients of the right of privacy on behalf of the Prophet Mohammad (pbuh).

3.6 The Role of Government

Privacy is not just an individual or religious affair; rather it is a right of the individual that has to be respected by the state and government.⁶⁴ For example, it is reported that:

During the Caliphate (rule) of Umar ibn al-Khatab, he used to go around on night patrol of the city of Al-Madinah. One night while on patrol, he heard some noise of drunkenness coming from a house and he knocked on the door to find out what it was but no one answered him. He then climbed over the wall and saw a drunken party inside; he shouted down and accused the homeowner of breaking the law prohibiting intoxicants. The man replied, "If I have committed one sin, you have committed four sins to find out. You spied on us

⁶³ Ibid 220.

⁶⁴ Hayat, above n 19, 140.

against God's command that 'spy not on each other', you climbed over the wall despite God's command that: 'enter houses through the proper doors', you entered without announcing yourself nor greeting in violation of God's command that: 'announce your presence and invoke greetings of peace upon those therein', you entered without permission in violation of God's command that 'do not enter until permission is given you.'" The Caliph Umar was abashed and he said: "You are right and I must forgive you your sin". The man then indicated the Caliph saying: "That is your fifth sin, you claim to be the Caliph and protector of Islamic law, how can you then say you forgive what God has prohibited".⁶⁵

This vividly illustrates the importance of the right to privacy under Islamic law and that the privacy of individuals cannot for any reason be violated contrary to due legal process.⁶⁶ It can be concluded that the above example given of the 'head of state' in the early stage of Islam illustrates the legal right to privacy and its application to all citizens, from the highest to the lowest. In this example, personal freedom and private affairs are also protected and advantaged over the public interests. Thus, the concept of privacy as discussed in the above chapter as the 'right to be let alone' has already been identified and explored 1400 years ago.

3.7 Concluding Remarks

This chapter has briefly examined the position of Islam towards the concept of privacy. The Islamic law fundamentally values the concept of privacy. This appears in many verses of the *Holy Qur'an* and the *Sunnah* which both emphasise human dignity and the honour of human beings.

⁶⁵ Ala'eddin Hendi, *Kanzu'l-Ummâl fi Sunan wa'l-Aqwal wa'l-Afal*, vol 3/808 Hadith; 8827.

⁶⁶ Mashood A Baderin, *International Human Rights and Islam* (2003) 117.

According to the *Shari'ah*, the right to privacy comes in two normative frameworks: prohibition of intrusion into another's privacy, and instructions and guidance for keeping secrets. Included in the first category is the prohibition against espionage, trespass and eavesdropping. The second category includes keeping secrets of others in the context of a marital relationship, personal sins, and information imparted to others in confidence. Within this framework, personal privacy has been considered as a fundamental human right.⁶⁷ Although, evidence from the *Qur'an* and the *Sunnah* address only certain aspects of the right of privacy, and are mentioned above, this does not mean that the right of privacy in Islam is restricted to only those aspects.

Relying on analogy, the right to privacy in Islam extends to new aspects that have accompanied the explosion of ICTs, such as the right to privacy in the use of information and communication technologies, the confidentiality of personal conversations by landline telephones, mobile telephones, satellite communications, and of other personal and corporate communications in the form of e-mails and faxes. Again, storage of the data generated and collected not only in hard copy but also in electronic databases must necessarily be subject to privacy protection.

The *Shari'ah* on privacy provides moral advice and religious guidance side by side with legal injunctions and makes respect for the privacy of others an integral part of the social and cultural ethos of the Muslim community, and

⁶⁷ Azmi, above n 36, 130.

this can, in turn, be expected to play a supportive role in legislation.⁶⁸ Such legislation may address the shortcomings of privacy in the context of the information and communications technology in Jordan as a predominantly Muslim country.

⁶⁸ Kamali, above n 20, 234.

Chapter Four

Privacy and Information and Communications Technology in Jordan: *The Public Sector*

4.1 Introduction

The Information and Communication Technology (ICT) sector has been one of the fastest growing sectors in Jordan. Its importance cannot be ignored, with ICT affecting every other sector in the Jordanian society, including telecommunications, education, banking, commerce, and employment. This chapter first examines the impacts of ICT in general and on privacy in particular. The chapter then examines ICT in the public sector by looking at e-government in Jordan. In an attempt to do this, an online study is carried out to determine the extent to which Jordanian governmental agencies have been aware of the issue of privacy and how they have addressed it. The chapter also provides an assessment of the individual privacy in the public domain regarding the use of ICT.

4.2 ICT and its social, economical and political impacts

It is widely recognised that ICT provides a number of socio-economic benefits, among them the improvement of business operations and public services, the reduction of poverty and the improvement of government performance.¹ The use of ICTs will improve the basic social services provided by the government to its citizens.² Education, for example, can be improved by the use the use of ICT to facilitate distance learning and the construction

¹ Ministry of Information and Communications Technology (MoICT), 'National ICT Strategy of Jordan 2007-2011' (Ministry of Information and Communications Technology, 2007) 1.

² Daniel Morales-Gomez and Melesse Martha, 'Utilising Information and Communication Technologies for Development: The Social Dimensions' (1998) 8(1) *Information Technology for Development* 3, 5.

and use of an on-line library.³ Healthcare can also be improved, for example, by the use of ICT to establish an electronic health record (EHR) to record health information, such as patient demographics, medical history, immunisations, laboratory data, procedures and surgeries, diseases, progress notes, medications, vital signs, and radiology reports. EHRs could incorporate information from any healthcare practice a patient uses and make this information easily accessible to other healthcare practitioners.⁴ In 2009, the Jordanian Government launched the national e-Health Programme 'Hakeem', which aims to establish a database of medical histories of patients across the country. The program seeks to minimise medical errors and provide accurate information on patients.⁵ In order to implement this program, the United States Trade and Development Agency (USTDA) has provided Jordan with assistance in the form of a grant of USD 567,600. Electronic Health Solutions, a non-profit company, is to carry out the implementation of this project.⁶

On the level of economics, ICT can play an important role in combating corruption and in making the operations of government institutions more transparent, by reducing the opportunities and incentives for, and increasing the costs of, corruption. By widely disseminating information about the

³ Cees J Hamelink, 'New Information and Communications Technologies, Social Development and Cultural Changes' (Discussion Paper No 87, United Nations Institute for Social Development, 1997) 14.

⁴ George W Reynolds, *Ethics in Information Technology* (2nd ed, 2007) 276.

⁵ Mohammad Ghazal, 'King Launches e-Health Plan', *The Jordan Times* (Amman), 1 November 2009, <<http://www.jordantimes.com/index.php?news=21113&searchFor=Hakeem#>> at 24 December 2010.

⁶ Ministry of Planning and International Cooperation, *US Grant for Feasibility Study on Electronic Health Records in Jordan* (2010) Ministry of Planning and International Cooperation <<http://www.mop.gov.jo/arabic/>> at 24 December 2010.

government's actual performance, it can also empower individual citizens and groups to hold government officials publicly accountable.⁷ Furthermore, ICTs can help reduce the pockets of poverty by facilitating contact among disadvantaged people and by helping put their issues and needs onto the national agenda, and so increase pressure on government for policies and services that address their needs. Just as importantly, ICTs can help the poor preserve and share their knowledge and cultures, and learn from each other about concrete ways to address their own challenges.⁸ In this context, the Government of Jordan (GOJ) launched an initiative in 2000 known as the 'Knowledge Station Initiative'. It aims to enable all segments of the Jordanian society, irrespective of their geographical location or economic status, to obtain the necessary skills in ICT that would allow them to become productive members of society.⁹

On the political level, ICT can increase the participation of citizens (particularly the young) in the decision-making in the public arena. A survey of political involvement in 19 European countries found that regular internet users were significantly more likely to be a member of a civil organisation, more likely to have taken part in product boycotts and signed petitions, and more likely to have donated to a political party.¹⁰ This suggests that ICT channels such as the internet may be used by young users as a means to

⁷ Kerry S McNamara, 'Information and Communication Technologies, Poverty and Development: Learning from Experience' (Background Paper for the infoDev Annual Symposium, 9–10 December 2003, Geneva, Switzerland, The World Bank, 2003) 59, avail <www.infodev.org> at 18 April 2009.

⁸ Ibid 63.

⁹ MoICT, *E-Initiative Database* (2003) Ministry of Information and Communications Technology (MoICT) <http://www.moict.gov.jo/MoICT/MoICT_Initiative.aspx> at 28 April 2009.

¹⁰ Naomi Halewood and Charles Kenny, 'Young People and ICTs in Developing Countries' (2008) 14(2) *Information Technology for Development* 171, 175.

engage in public policy decision making. In Jordan, for instance, users of the well-known social network 'Facebook' number about 883,780 as of May 2010. More than 70 per cent of those users are under the age of 25.¹¹ A number of these users are creating groups on the network to lobby against government policies.

Advances in the development and use of ICTs have resulted in a number of concerns being raised in relation to privacy. The following section examines the ICT and its impacts on privacy.

4.3 ICT and its impact on privacy

ICT can be used to facilitate the collection, aggregation, systematisation and mining of vast amounts of information. Such information may be acquired from large numbers of individuals, with or without their consent, or in some cases without their awareness.¹² Personal information may be initially gathered for a legitimate purpose (for example, processing a loan or credit card application, filling out a warranty card or applying for health or life insurance),¹³ but then later used for unauthorised purposes. The unauthorised use of personal information raises concerns regarding the invasion of privacy.¹⁴

¹¹ Spot On Public Relations, *Middle East and North Africa Facebook Demographics* (2010) Carrington Malin <http://www.spotonpr.com/wp-content/uploads/2010/05/FacebookMENA_24May10.pdf> at 22 December 2010.

¹² Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008) 150.

¹³ Sandra Byrd Petersen, 'Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?' (1995) 48 *Federal Communications Law Journal* 163, 171.

¹⁴ Joseph Migga Kizza, 'Anonymity, Security, Privacy and Civil Liberties' in David Gries and Fred B Schneider (eds), *Ethical and Social Issues in the Information Age* (3rd ed, 2007) 114.

The use of personal information for illegitimate purposes can affect individuals who provided the information. The unauthorised use may have adverse effects on the person's employment, career choices and financial situation.¹⁵ For example, most people consider their medical records particularly private. Information they contain may be particularly sensitive: a record of sexually transmitted diseases, a termination of pregnancy undisclosed to parent or partner, alcoholism or previous drug abuse. The unauthorised disclosure of such information could lead to discord or breakdown of a relationship (in regard to STD or termination information); or loss of employment or potential employment, and an inability to obtain insurance (in regard to alcohol or other substance abuse information or even information regarding genetic predisposition to particular conditions).¹⁶ This has been seen to have occurred in a number of developed countries until adequate legislation was introduced to restrict or eliminate such practices.¹⁷

In some cases, records of purchase of services have allowed persons to be targeted for marketing campaigns. In one instance this involved continued mail outs regarding pregnancy (including birthday cards) long after the woman concerned had suffered a miscarriage, and caused her and her family

¹⁵ Michael Erbschloe and John Vacca, *Net Privacy: A Guide to Developing and Implementing an Ironclad eBusiness Privacy Plan* (2001) 3.

¹⁶ James Rachels, 'Why Privacy is Important' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 290, 291.

¹⁷ Lawmakers in the United States passed the Health Information Technology for Economic and Clinical Health Act, (HITECH) (HR 1§§ 13101-13424) in 2009 as part of the stimulus legislation. The new law significantly expands security and privacy protections under the *Health Insurance Portability and Accountability Act* of 1996. HITECH became effective on 17 February 2010. See <<http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202431306531>> at 22 December 2010.

intense and prolonged distress.¹⁸ In another instance within a month of receiving hospital treatment for prostate cancer, a US patient was targeted in a pharmaceutical company mail out on their particular cancer medication. Again these are examples of what can occur in the absence of strict guidelines and adequate legislation.¹⁹

Furthermore, David Holtzman believes that individuals can be affected when technology is given the power to make decisions that are based on, or that lead to, violations of their privacy. Holtzman argues that 'individuals will be labeled based on personal information that is analyzed by machines, not by human beings'.²⁰ For example, stores are now able to track individual customer purchasing patterns by using information gathered from customer use of store-based charge cards, credit cards and other methods of cash-free payment. The information can be used for targeted promotions, and details on-sold for use for other purposes, such as by insurance companies who may purchase data on a potential insured to conduct a risk analysis on the basis of the person's purchases (dietary habits, including red meat and alcohol consumption).²¹

The above examples show that individuals are under constant surveillance by advanced technological devices that have the ability to categorise them based

¹⁸ Petersen, above n 13, 167, where the author cites R J Ignelzi, 'Mail and Telejunk: US Marketers have Your Number; Your Age and Your Shoe Size too' *San Diego Tribune*, 4 July 1995, E1, E4.

¹⁹ Harry Henderson, *Privacy in the Information Age* (1999) 26.

²⁰ David H Holtzman, *Privacy Lost: How Technology Is Endangering Your Privacy* (First ed, 2006) 48.

²¹ Petersen, above n 13, 168. Indeed as she reveals, in the United States, '[a]n insurance company can combine this information with medical records that can be obtained from the medical information Bureau (MIB) which has data on 15 million people [of the US and Canada]. The result a very complete picture of a person's lifestyle, regardless of whether or not the information is accurate': 168.

on personal information collected from different sources. While the information collected concerns some of the most sensitive details of personal life, individuals may be unaware of its existence and, therefore, unable to correct or amend any errors contained in this information.²²

4.4 ICT in Jordan

Jordan has transformed itself from a rural, poor country to a developing urban country with a highly educated population, with a literacy rate of 92.3 per cent as of year 2008. Jordan has a young population, 70 per cent of the total population (about 4.09 million) is under the age of 30.²³ Jordan's higher education institutions, comprising 8 public universities, 12 private universities, and 21 community colleges accommodate over 120,000 students. The number of IT students is currently 8,000 at the university level and 5,300 at the college level. Jordan has the highest proportion of university graduates in technological fields among the countries in the region.²⁴

The ICT sector enjoys strong support from His Majesty King Abdullah II through his appointed government. Progressive regulatory and policy reform is underway while the sector is being transformed under an ambitious privatisation plan.²⁵ A number of factors — including highly qualified human resources, the availability of world-class infrastructure, and the success of Jordanian IT companies — contribute to the growth of Jordan's ICT sector

²² Ibid 169.

²³ Department of Statistics, *Jordan in Figures: Selected Indicators (2008)* Department of Statistics - Government of Jordan <http://www.dos.gov.jo/dos_home_e/main/jorfig/2008/jor_f_e.htm> at 23 December 2010.

²⁴ MoICT, *Invest in ICT in Jordan (2005)* Ministry of Information and Communications Technology <<http://www.jordanecb.org/pdf/InvestinICTinJordan.pdf>> at 16 April 2009, 8.

²⁵ Ibid.

and help the transformation of Jordan into a major regional IT hub.²⁶ The growth of this sector, locally and regionally, provides attractive opportunities for foreign investors.

The ICT sector in Jordan is thriving and has become a major contributor to the growth of the Jordanian economy.²⁷ According to a report by the World Economic Forum, Jordan's Networked Readiness Index (NRI) has improved, and in 2010 it ranked 44th of the 103 countries surveyed. The NRI is the scale that assesses the extent to which different countries benefits from the latest ICT advances.²⁸ In 2003, the revenues from the IT sector in Jordan were USD 295.9 million and reached USD 895 million in 2009 (see Table 1 below). Revenues from the telecommunications sector were USD 1.3 billion in 2009 (see Table 2 below) and, based on conservative assumptions, the Ministry of Information and Communications Technology (MoICT) estimates that revenues from the Jordanian ICT sector will reach USD 3 billion by 2011. In addition, employment in the ICT sector will grow in tandem to revenue growth. The MoICT estimates that employment in the sector will rise to 35,000 in the period 2010–2011.

²⁶ MoICT, 'Research & Development Strategy for Information and Communication Technology 2007-2010' (2007) 1, Ministry of Information and Communications Technology <www.moict.gov.jo> at 16 April 2009.

²⁷ MoICT, *Invest in ICT in Jordan*, above n 24.

²⁸ World Economic Forum, 'The Global Information Technology Report 2009-1010: ICT for Sustainability' (The World Economic Forum, 2009) <http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf> at 23 December 2010.

Table 1**ICT Growth in Jordan (2003-2009)**

	2003	2004	2005	2006	2007	2008	2009
IT Export Revenues	\$69,728,000	\$79,410,743	\$162,619,518	\$191,520,379	\$196,907,691	\$226,863,277	\$209,526,864
Growth	74.16%	13.89%	105%	17.80%	2.81%	15.21%	-7.64%
IT Domestic Revenues	\$226,183,000	\$361,103,905	\$418,254,125	\$578,554,212	\$686,063,063	\$735,571,817	\$685,461,382
Growth	20.02%	59.65%	15.80%	38.33%	18.58%	7.22%	-6.81%
IT Total Revenues	\$295,910.00	\$440,514,648	\$580,873,643	\$770,074,591	\$882,970,754	\$962,435,094	\$894,988,247
Growth	29.51%	48.87%	31.86%	32.5%	14.66%	9.00%	-7.01%
IT Foreign Direct Invest. (FDI) Yearly	\$11,594,500	\$2,900,000	\$10,524,761	\$13,569,656	\$3,070,791	\$1,690,141	\$16,231,326
IT Employment	8,117	8,523	10,032	10,712	11,034	10,294	11,334

Table 2**Telecommunications Sector Revenues in Jordan Figures year 2009**

	Domestic	Export	Total
Telecommunications Revenues	\$1,288,298,369	\$11,618,624	\$1,299,916,994

Source: int@j-ICT & ITES Industry Statistics & Yearbook 2009, int@j

The (MoICT) in cooperation with other Ministries, donor programs and non-governmental organisations in Jordan, has undertaken various ICT related initiatives.²⁹ One of the most important initiatives adopted by policy makers in Jordan, and one which will be examined shortly, is the ‘Electronic Government initiative’ (e-government). However, it is worthwhile to briefly summarise aims and goals of other initiatives and projects implemented by the Government of Jordan in order to shed light on ICT developments in Jordan. These initiatives and projects include:

1. **The ‘e-Village Project’:** This project began in July 2006 and ‘seeks to address the need to increase the capacity, awareness and economic opportunities of rural women in the field of ICT’.³⁰ Its main objectives are:

- (1) to raise villagers’ awareness and to enhance internal communications among villagers through establishing an “Information and Awareness Centre”,
- (2) to build the capacity and professional skills of the village citizens to allow them to benefit from different IT services and opportunities created by the project through establishment of an “Empowerment Centre”, and
- (3) to enhance the economic opportunities within the village through creating new job opportunities ... within the “E-Service Centre”.³¹

2. **The ‘Connecting Jordanians Initiative’:** This initiative ‘aims to coordinate and accelerate critical developments and reforms intended to make ICT an important facet in the lives of all Jordanians and to improve their economic, social and cultural prospects in meaningful ways’.³² A concrete example of this is the plan to provide computers and broadband Internet access to all of the 3000 Jordanian primary and secondary schools

²⁹ MoICT, *E-Initiative Database*, above n 9.

³⁰ Ibid.

³¹ Ibid.

³² Ibid.

by 2010. As a result, teachers in these schools are required to take the International Computer Driving Licence, a project financed by the United Nations to promote the creation of basic IT skills.³³

3. **Laptop ‘Note Book’ for every University Student:** This aims ‘to bridge the country’s digital gap and support the usage of ICT tools in the educational process by providing a laptop for each university student in the Jordanian public and private universities at an affordable cost’.³⁴ Internet access and wireless technologies are also to be supplied. This initiative also aims to help transform the Jordanian economy into an e-economy by increasing technology use and by providing training for the workforce in the country.

4. **Jordan’s Broadband Learning Network:** This initiative launched in January 2003 aims to achieve the following goals:

- (1) promoting collaborative learning programs, (2) enabling access to learning content for all Jordanians and contributing to lifelong learning opportunities, (3) supporting a wider range of broadband services, including multimedia rich content, (4) promoting the development of a cluster of e-Learning content, applications, and services of regional and global export meeting the network requirements of speciality users, and (5) stimulating the development of the “Knowledge Economy”.³⁵

The most interesting initiative regarding the privacy issue in the context of ICT is the Jordanian e-government initiative. The focus on this initiative is significant for a number of reasons. First, in Jordan the public sector is the

³³ Claudio Ciborra and Diego D Navarra, 'Good Governance, Development Theory, and Aid Policy: Risks and Challenges of E-Government in Jordan' (2005) 11(2) *Information Technology for Development* 141, 150.

³⁴ MoICT, *E-Initiative Database*, above n 9.

³⁵ *Ibid.*

largest employer, being the most important economic entity.³⁶ Second, launching an e-government portal involves fundamental changes in the culture and operating practices of government and the perception of government by both citizens and businesses, as e-government is based on the view of government as a supplier of services and citizens or businesses as its clients. Third, as the e-government portal becomes a major link between public sector and citizens and/or businesses, the portal will become the largest single entity in terms of an information database. It has the ability to collect, access, store, and transfer vast amounts of personal information. The issue of privacy in the context of e-government in Jordan will be examined in detail below.

4.4.1 Electronic Government in Jordan

The Organisation for Economic and Co-operation Development (OECD) has defined 'e-government' as the 'use of information and communication technologies and particularly the Internet, as a tool to achieve better government'.³⁷ E-government aims to make the interaction between government and citizens (G2C), government and business enterprises (G2B), and inter-agency relationships (G2G) more friendly, convenient, transparent and inexpensive.³⁸

³⁶ Claudio Ciborra, 'Interpreting E-government and Development: Efficiency, Transparency or Governance at a Distance?' (2005) 18(3) *Information Technology and People* 260, 262.

³⁷ Organisation for Economic Co-operation and Development (OECD) *The e-Government Imperative* (2003) 11.

³⁸ Subhajit Basu, 'E-Government and Developing Countries: An Overview' (2004) 18(1) *International Review of Law Computers and Technology* 109, 113.

The development of this interaction, however, can be divided into five stages.³⁹ The first stage is called 'emerging'. At this stage, the government creates a web page or an official website, links to ministries and departments (for example, education, health, labour and finance). Much of the information provided in this stage is static (for example, the contact details of ministries or departments) and there is little interaction with citizens.⁴⁰ The second stage is called 'enhanced'. The government provides more information on public policy and governance. Links are created to archived information that then becomes easily accessible to citizens. This information includes, but is not limited to, documents, forms, reports, laws and regulations and newsletters. The third stage is called 'interactive'. The government at this stage delivers online services such as downloadable forms for tax payments and applications for passport renewals. The fourth stage is called 'transactional'. At this stage the government begins to transform itself by introducing two-way interactions between 'citizens and government'. This stage involves options for paying taxes, applying for ID cards, birth certificates, passports and licence renewals, as well as other similar G2C and C2G interactions, and allows the citizens to access these services online 24/7. All transactions are conducted online. 'Connection' is the fifth stage, where government transforms itself into a connected entity that responds to

³⁹ The description here of the five stages relies heavily upon a UN publication: UN Department of Economic and Social Affairs, 'United Nations e-Government Survey 2008: from E-Government to Connected Governance' (United Nations, 2008) 16
<<http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf>>.

⁴⁰ See, the Official Site of the Jordanian e-Government, avail <<http://www.jordan.gov.jo>> at 23 December 2010.

the needs of its citizens by developing an integrated back office infrastructure.⁴¹

The United Nations e-Government Survey in 2008⁴² placed Jordan 50th on the e-Government Readiness Index,⁴³ recording an improvement from its 68th ranking in 2005.⁴⁴ In regards to the E-Participation Index, surprisingly, Jordan recorded the greatest move upwards, from being ranked 90th in 2005 to 15th in 2008. E-participation can have a number of ramifications for governance.

E-participation is a tool that enables governments to dialogue with their citizens. By enhancing government's ability to request, receive and incorporate feedback from citizens, policy measures can be better implemented to meet the needs of citizens and provide them with suitable services.⁴⁵

The above results indicate that Jordan is confidently committed to interact with its citizens with most advanced technology channels including the technology of e-government.

The national e-government initiative, launched in the year 2000 by the Government of His Majesty King Abdullah II, aims to transform the nation

⁴¹ UN Department of Economic and Social Affairs, 'United Nations e-Government Survey 2008', above n 39, 16.

⁴² The United Nations e-Government Survey 2008 presents a comparative assessment of the 192 United Nations Member States. 'The Survey evaluates the application of information and communication technologies by governments. The aims to which these technologies are put to use vary, but include: better access and delivery of services to citizens, improved interaction with citizens and business, and the empowerment of citizens through access to information ... This evaluation of e-government readiness places citizens at the forefront, by focusing on the governmental services and products that primarily affect them': UN Department of Economic and Social Affairs, 'United Nations e-Government Survey 2008', above n 39, 12.

⁴³ The e-government readiness index measures the capacity of governments to develop and implement e-government services. The index ranges from 1 (low level of readiness) to 1 (high level). The indicator has three sub-indices: web measure, telecommunication infrastructure and human capital. Jordan's e-government readiness index is 0.5480 for the year 2008: UN Department of Economic and Social Affairs, 'United Nations e-Government Survey 2008', above n 39, 14.

⁴⁴ Ibid 35.

⁴⁵ Ibid 58.

into a knowledge-based society based on a competitive and dynamic economy.⁴⁶ The e-government initiative is administered by a committee comprising eight members selected from both the public and private sectors. The committee has been chaired from the outset by a representative of the then newly formed MoICT. The Ministry is responsible for formulating telecommunication policy and coordinating e-government initiatives, as well as attracting investment in the ICT sectors, and setting the ICT policy and strategic plan for the telecommunication and postal sector.⁴⁷

Despite all government agencies in Jordan (for example, ministries and departments) being virtually located in one portal (Jordan's e-government website), each government agency is still in charge of its own ICT policies.⁴⁸ This means that each agency has its own method of collecting, accessing, using and disclosing personal information obtained from individuals. In regard to individual privacy protection, each agency is able to lay down its own policies and guidelines. This may result that in a conflict between policies and guidelines when there is a breach of individual privacy. For instance, government agencies in Jordan are not bound by the legal terms and conditions included within the privacy policy located in the e-government portal. Supplying personal information to an agency through the e-government portal does not guarantee this information is protected by the agency in accordance with the terms and conditions stated in the e-

⁴⁶ Government of Jordan, *e-Government Program* (2006) Government of Jordan <www.jordan.gov.jo> at 30 April 2009.

⁴⁷ Ciborra, above n 36, 263.

⁴⁸ Yousef Elsheikh, Andrea Cullen and Dave Hobbs, 'e-Government in Jordan: Challenges and Opportunities' (2008) 2(2) *Transforming Government: People, Process and Policy* 83, 89.

government privacy policy. The following sections highlight the issue of privacy in the Jordan's e-government context.

4.4.2 E-Government Initiative and Individual Privacy Concerns

The lack of privacy protection might inhibit the achievements of the e-government project. If individuals are not confident that their privacy is adequately protected, they will be reluctant to use the available e-government services.⁴⁹ A study conducted by Hart-Teeter Research found that 60 per cent of Americans who use the internet are interested in using e-government for various activities, such as filing a change of address, obtaining birth certificate or renewing driver's licence. However, nearly 45 per cent of Americans believe that submitting their personal information to government web sites may risk the security and privacy of that information.⁵⁰ Due to a lack of similar studies in Jordan, the author uses a different method to assess the level to which individual privacy is protected and maintained in the context of e-government. The so-called 'Fair Information Practices' (FIPs) principles are used as a bench mark for privacy assessment in Jordan. The use of FIPs as a bench mark is justified on the basis of a number of factors.

⁴⁹ Priscilla M Regan, 'Privacy in an Electronic Government Context' in Hsinchun Chen et al (eds), *Digital Government: E-Government Research, Case Studies, and Implementation* (2008) 128.

⁵⁰ PA Times, 'E-Government Study Finds Ease, Engagement, Privacy, Protection are Top Priorities', *PA Times* 26(5) (Washington, DC), May 2003, 2, avail <www.aspanet.org> at 21 May 2009.

First, FIPs were proposed in 1973 by the US Department of Housing, Education, and Welfare (HEW)⁵¹ and aimed to address the inadequacy of protection for privacy in the US health sector. The HEW proposal report made a strong influential statement in relation to privacy concerns in the context of government information stored in computer databases. The HEW report states:⁵²

It is no wonder that people have come to distrust computer based record keeping operation. Even in non-governmental settings, and individual's control over the personal information that he gives to an organisation or that an organisation obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused. There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays, an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers-unknown, unseen, and all too frequently, unresponsive. Sometimes the individual does not even know that an organisation maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination or challenge its use by others.

To address these privacy concerns regarding the use and collection or personal information by the government, the HEW report suggested that the FIPs to be implemented:⁵³

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.

⁵¹ US Department of Health Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973) HEW <<http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>> at 16 February 2011.

⁵² Ibid.

⁵³ Ibid.

3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.
5. Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Since then, FIPs have been widely used as a standard benchmark for privacy protection evaluation.⁵⁴ For example, the ‘privacy policy’ located on the US e-Government portal⁵⁵ uses FIPs as a benchmark for privacy protection. The US e-Government portal is ranked by the UN as the undisputed world leader in e-government readiness.⁵⁶

Second, as noted above in Chapter two, the OECD has built its privacy guidelines based on FIPs as they are embodied in the OECD Guidelines. While the OECD Guidelines are viewed as set of recommendations rather than legal binding requirements for its members, Jordan (a non-member state) could use the OECD privacy guidelines for privacy protection.

Finally, the US Federal Trade Commission (FTC) has developed FIPs into five main principles which have become the most popular benchmark for evaluating the adequacy of privacy protection for the online environment.

⁵⁴ United States Government Accountability Office, 'Privacy: Key Challenges Facing Federal Agencies' (United States Government Accountability Office, 2006) 4, available <www.gao.gov> at 15 June 2009.

⁵⁵ Initially <www.firstgov.gov>, now <www.usa.gov>. For policy, see US Government, *Privacy and Security* (2010) US Government <http://www.usa.gov/About/Privacy_Security.shtml> at 24 December 2010.

⁵⁶ Department of Economic and Social Affairs, 'Global E-Government Readiness Report 2005: From E-Government to E-Inclusion' (United Nations, 2005) 31.

These principles are being implemented in the US-EU Safe Harbour Framework (mentioned earlier), which aims to close the gap of privacy approaches between the US and the EU. This agreement will be discussed in detail in Chapter Eight.

The online privacy principles developed by the FTC to assess the adequacy of privacy protection include the following:⁵⁷

1. *Notice / Awareness*: Individuals should be given notice of an entity's policies regarding individual privacy protection prior to the collection of personal information from them. This principle is significant as individuals are then more able to make an informed decision as to whether and to what extent they may disclose personal information.

The FTC, for example, has noted that among the 'essential' material to be disclosed to the individual prior to collection of data are the 'identity of the entity collecting the data,⁵⁸ the uses to which the data will be put,⁵⁹ the identity of any potential recipients of data,⁶⁰ and 'the nature of the data collected and the means by which it is collected'.⁶¹ Such material is to be included in the notice to ensure that individuals are properly aware of the

⁵⁷ Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) Federal Trade Commission <<http://www.ftc.gov/reports/privacy3/priv-23a.pdf>> at 4 March 2010, 7–8.

⁵⁸ Ibid 7. The FTA cites a number of documents for this principle including: *OECD Guidelines – Openness Principle*, *EU Directive* art 10 and FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, Staff Report (December 1996) 9-10.

⁵⁹ Federal Trade Commission, *Privacy Online*, above n 57, 7. The FTA cites a number of documents for this principle including: *OECD Guidelines – Purpose Specification Principle*, *EU Directive* art 10 and FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, Staff Report (December 1996) 9-10. The FTC notes that data collected should not be used for other purposes without the data provider's consent: 49.

⁶⁰ Federal Trade Commission, *Privacy Online*, above n 57, 7. The FTC here cites *EU Directive* art 10.

⁶¹ Ibid 8. The FTC here cites the US Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995) 21.

information being collected about them.⁶² The FTC also notes that individuals are to be informed as to whether the supply of the information requested is compulsory or voluntary and the consequences of failure to supply the requested information.⁶³

2. *Choice / Consent:* Individuals are to be given the option to determine how personal information collected from them may be used.⁶⁴ For example, individuals who provide their personal information to governmental agency (for example, health department) may wish that this information not to be used by another governmental agency (for example, the social security department), or to be used externally by a third party (for example, an insurance company).

3. *Access / Participation:* Individuals should be able to access information collected about them to ensure that this information is accurate and complete. For example, individuals should be given the right to view (access) their information kept by a governmental agency. If this information or some part of it is inaccurate and/or incomplete, individuals should have the right to contest the data to ensure correction and/or amendment of their information.⁶⁵

4. *Integrity / Security:* Information collected about individuals is to be accurate and secure. Therefore, data collecting entities must take reasonable steps to ensuring the integrity and safety of personal information. For example, in relation to data integrity, agencies should use only reputable

⁶² Federal Trade Commission, *Privacy Online*, above n 57, 7.

⁶³ Ibid 8. The FTC cites, among a number of materials, EU *Directive 10*.

⁶⁴ Federal Trade Commission, *Privacy Online*, above n 57, 8.

⁶⁵ Ibid 9.

sources of information, cross-reference information against multiple sources, provide access to information for concerned individuals, and delete unnecessary information.⁶⁶ In regard to security, measures should be taken for example to limit access to data to authorised persons for authorised purposes only, as well as heightening security through the use of data encryption for storage and transfer.⁶⁷

5. *Enforcement / Redress*: The above principles cannot be effective in ensuring privacy protection unless there is an enforcement mechanism to enforce and implement these principles. Lack of a mechanism for enforcement and redress would result in seeing the above principles as set of suggestive principles rather than legal requirements.⁶⁸

Enforcement may take different forms in different countries. For example, the US believes generally in a self-regulatory regime⁶⁹ while, the EU views comprehensive legislation as a suitable approach to ensure individual privacy protection. Both regimes will be discussed throughout this research.

With respect to Jordan's position towards the above principles, and in order to evaluate individual privacy protection against these principles, a case study was conducted involving a number of government agencies in Jordan with an online presence (websites). Forty governmental websites were visited through the official Jordanian e-government portal

⁶⁶ Ibid 10.

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ An exception appears to be the *Children's Online Privacy Protection Act* of 1998, 15 USC §§ 1301-1308. See <<http://www.ftc.gov/ogc/coppa1.htm>> at 14 January 2011. This Act applies to persons under 13 years of age.

(www.jordan.gov.jo) between 4 of June 2009 and 10 June 2009. The intention here is to assess the level to which the privacy of personal information is protected by government agencies. The selection of the e-government portal in Jordan for this case study is due to the fact that this portal is the access point for the largest single entity with the ability to collect, process, access and transfer personal information. This case study also aims to examine the following issues:

- a) The number of government agencies that have privacy policy/statement on their websites, and
- b) The content of these privacy policy/statements, if they are available, and their standards as compared to the FIPs model.

From Table 3 'Government Agencies with an Online Presence in Jordan' (further below), two major issues have been identified that present a real challenge to individual privacy protection in Jordan, namely the collection of personal information and the use and disclosure of such information. These issues are discussed below.

4.4.2.1 Collection of Personal Information

The collection of personal information concerning individuals has always invoked issues of privacy. Online technologies increase privacy concerns because they allow for faster and, easier storage of more data, as well as aggregation of the data, possibly without the individual's consent.⁷⁰ In relation this privacy issue, the current case study reveals that websites run

⁷⁰ France Belanger and Janine S Hiller, 'A Framework for e-Government: Privacy Implications' (2006) 12(1) *Business Process Management Journal* 48, 54.

by all Jordanian government agencies have the ability to collect personal information. The collection can be made in different methods but appears to be direct. The icons ‘contact us’, ‘suggestions and complaints’, and ‘apply for service’ located on the front page of the government websites allow individuals to submit their personal information when contacting the relevant department.

As far as privacy protection is concerned, only three government agencies of the forty surveyed provide a ‘privacy policy/statement’ on their websites. Table 4 (further below) shows the three websites: the Official Site of the Jordanian e-Government,⁷¹ the Telecommunications Regulatory Commission (TRC)⁷² and the Royal Jordanian Airlines.⁷³ An examination of the privacy policies of these websites allows the following observations to be made.

First, it is believed that these three websites have voluntarily chosen to place their privacy notification and not because they were required to do so by Jordanian law or regulation. If they were required by a law or regulation, the remaining websites would have similarly exhibited privacy policies.

Second, the terms and conditions included in the privacy policies of these websites differ. Individuals who visit one website may become confused with regard to privacy policy when visiting another website; and may have a

⁷¹ See Appendix A, Exhibit 1 of the Government of Jordan, *Privacy Policy (2009)* The Government of Jordan <www.jordan.gov.jo> at 4 June 2009.

⁷² See Appendix A, Exhibit 2 of the Telecommunications Regulatory Commission, *Privacy Policy (2009)* Telecommunications Regulatory Commission <www.trc.gov.jo> at 4 June 2009.

⁷³ See Appendix A, Exhibit 3 of the Royal Jordanian, *Privacy Policy (2009)* Royal Jordanian Airlines <www.rj.com> at 4 June 2009.

different understanding of policy when that knowledge is compared to that of another person who has visited a different website. Below are two examples regarding differences in the contents of privacy policy.

Example one: Unlike the e-Government of Jordan and the Royal Jordanian Airlines websites, the TRC provides a definition to the terms of ‘personal information’. On the ‘privacy policy’ hyperlink located on the ‘home page of the TRC website, ‘personal information’ is defined as:

Any information that may be used to identify an individual, including, but not limited to, a first and last name, email address, a home, postal or other physical address, other contact information, title, industry, and other such information.⁷⁴

The author believes that the above definition has no legal basis in Jordanian law; the legal source of this definition is unknown. The only source detected that may be linked to this definition is found in US law. In section 1303(8) of the *US Children’s Online Privacy Protection Act* (COPPA), ‘personal information’ is defined as: ‘individually identifiable information about an individual collected online, including: first and last name, home and other physical address, e-mail address, telephone number, and any other information...’⁷⁵

It seems that the TRC has copied the US definition onto its own website. However, the difference between these two definitions is that the TRC’s definition is nothing more than terms included within a legally non-binding

⁷⁴ Telecommunications Regulatory Commission, *Privacy Policy* (2009) Telecommunications Regulatory Commission <www.trc.gov.jo> at 4 June 2009.

⁷⁵ *Children’s Online Privacy Protection Act of 1998*, 15 USC §§ 6501-6506.

policy. By contrast, the US law will determine whether the information is ‘personal information’ or ‘non-personal information’.

Example two: Point 5 of the privacy policy which is posted on the Jordanian e-government website provides a clear statement that the site will not use ‘cookies’ technology to track individuals who visit the site.⁷⁶ If this type of technology is to be used, the website will notify individual so they can accept or refuse it. In contrast, the website of the Royal Jordanian Airlines says ‘cookies’ technology will be used, but it will not sending an individual notification⁷⁷ to those utilising the site. It thus provides a ‘blanket’ notice in its policy. (It should perhaps be noted that in the US posting such a notice on a website appears to be the minimum required to satisfy the FTC privacy protection requirements.⁷⁸) In the TRC privacy policy statement, however, there is no statement on the use of ‘cookies’ technology.

The use of ‘cookies’ by a website is often seen as an invasion of privacy (particularly when their use is not indicated to the site user) as they have the capacity to build a profile on the needs, preferences and patterns of expenditure of any individual visiting particular websites. ‘Cookies’ work by placing an identifying code on the hard drives of those who visit the site. This code allows the visitor to be tracked as they travel through the website and to be recognised on subsequent visits.⁷⁹ The use of ‘cookies’ may cause

⁷⁶ See Appendix A, Exhibit 1.

⁷⁷ See Appendix A, Exhibit 3.

⁷⁸ Federal Trade Commission, *Privacy Online*, above n 57, 8.

⁷⁹ Basu, above n 38, 124.

harm to individuals. Potential problems include identity fraud, physical injury, financial hardship or harm to or his/her reputation.

In this context, it is important to distinguish two separate types of information that can be stored in 'cookies': personally identifiable information (PII) and non-personally identifiable information (non-PII). PII consists of information that is used to identify an individual such as: name, address, phone number, e-mail address, credit card number, social security number or identification number or national identification number or card (where applicable).⁸⁰ By contrast, non-PII is not directly linked to a particular person, with information collected anonymously (for example, statistical information, gender, race, purchases, or salary).

4.4.2.2 Use and Disclosure of Personal Information

The main issue regarding the use and disclosure of personal information in the online environment is that of consent. Personal information which has been collected by a government agency via its website may be transferred to another agency or even to a third party (non-governmental entity).⁸¹ Table 3 below indicates that all government agencies in Jordan have the ability to collect personal information. It also shows that they have the ability to use and disclose this information. In the context of e-government in Jordan, government agencies do not offer individuals any opportunity to give or

⁸⁰ Frederic Debusseré, 'The EU-E-Privacy Directive: A Monstrous Attempt to Starve the Cookies Monster?' (2005) 13(1) *International Journal of Law and Information Technology* 70, 77. See also, European Commission, 'PIN' 1 September 2009 (modified 25 November 2009) <ec.europa.eu/social/BlobServlet?docId=4225&langId=en> at 11 January 2011.

⁸¹ Maeve McDonagh, 'E-Government in Australia: the Challenge to Privacy of Personal Information' (2002) 10(3) *International Journal of Law and Information Technology* 327, 331.

withhold their consent to information collection and further dissemination. The FTC suggests two types of consent: 'opt-in' or 'opt-out'. The 'opt-in' method requires affirmative steps by the individual to allow the use, and disclosure of his/her personal information.⁸² Opt-in grants individuals (before they supply requested information) the opportunity to say 'yes', 'I approve' or 'I accept' to indicate whether their information is to be used or shared.⁸³ In contrast, the 'opt-out' method requires affirmative steps to *prevent* the collection, use and disclosure of such information.⁸⁴ This method allows unlimited information practices unless and until an individual says 'stop'.⁸⁵

In respect to the three websites that have privacy policies/statements (as shown in Table 4), a number of observations can be made regarding privacy principles of consent, access, security and enforcement.

In relation to the matter of consent, the findings reveal that all three websites do not use similar terms regarding how collected personal information about individuals may be used nor do they contain similar provisions. This may be due to each type of industry requiring a different privacy policy.

In respect to the principle of access, only the TRC website grants individuals the right to access to their personal information to ensure its accuracy.

⁸² Federal Trade Commission, *Privacy Online*, above n 57, 9.

⁸³ Mike Hatch, 'The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century' (2001) 27 *William Mitchell Law Review* 1457, 1494.

⁸⁴ Federal Trade Commission, *Privacy Online*, above n 57, 9.

⁸⁵ Hatch, above n 83, 1494.

Individuals can contact the TRC through an e-mail address or via a telephone number to advise of any changes or amendments to their personal information stored by the TRC.

In regards to the principle of security, all three websites claim to take all reasonable steps to ensure that the information collected is accurate and up-to-date. For example, the Jordanian e-Government privacy policy states that information that is out of date will be destroyed, deleted, or converted to an anonymous form of information.

Finally, with respect to the principle of enforcement, only the TRC privacy policy states that matters and disputes that may arise concerning the use of TRC site shall be governed by the Jordanian law, and the courts of Jordan should have jurisdiction to deal with these matters and disputes.

Based on the above findings, the author's analysis can be summarised as follow:

1. The government agencies in Jordan that do not have privacy policies/statement on their websites (37 of the 40) have the ability to use and disclose personal information that has been collected about individuals. These agencies are under no legal obligation to provide statements explaining their information privacy practices. As a result, the author believes that the use and disclosure of personal information by these agencies can be undertaken without an individual's consent.

2. The government agencies listed in Table 4 that do have privacy policies for their websites, do not provide clear information regarding the following:

a) Individual consent: government agencies are not required — based on their privacy policies — to obtain an individual's consent when collecting personal information. The author suggests that government agencies should not offer individuals an 'opt-out' option as it cannot be effective to adequately protect individual personal information. To be effective the 'opt-out' option relies upon individuals being able to understand how government agencies are using, disclosing and sharing their personal information. This is an almost impossible demand as individuals generally lack knowledge of the possible uses an entity can make of the information collected nor can all such possibilities be foreseen, even by the entities themselves at the time of the information being collected. It also relies upon individuals being informed that they have a right to opt-out of this information practices (using, disclosing and sharing).⁸⁶ The 'default setting, however, is of total freedom for the entity collecting the information in regard to its use, further disclosure (sharing internally or with external entity for related or unrelated matters) and so forth. The individuals' lack of control over their personal information leads the author to conclude that the 'opt-out' method cannot be effective. The three privacy policies listed in Table 4 do not provide individuals with

⁸⁶ Ibid 1495. Those contributing information also need to know that they can do so at any given point or at various points where they may not wish to disclose information or allow information disclosed to be shared.

options to consent regarding whether and how personal information may be used for purposes beyond those for which the information was provided.⁸⁷ And in regard to access by individuals to material they have supplied and the right to amendment of inaccuracies, none of the government agencies surveyed offered individuals the ability to access, view or delete their information. Individuals may thus be misrepresented in the data collected from or about them (for example in out of date or erroneous material that remains in an entity's records).⁸⁸

b) Individual complaint: privacy policies for government agencies listed in Table 4 do not provide clear information about complaint procedures and remedies for injured individuals. The lack of information on this issue makes privacy policies useless as individuals will question who is responsible for protecting their privacy and be suspicious regarding the entire issue.

c) Enforcement: privacy policies on these government websites do not state which government agency is in charge of enforcing their privacy rights. The simple reason is that Jordan has no specialised agency to enforce privacy rights. The enforcement provisions included in the TRC privacy policy are concerned with matters arising from the use of TRC website rather than its privacy policy.

⁸⁷ David L Baumer, Julia B Earp and J C Poindexter, 'Internet Privacy Law: A Comparison between the United States and the European Union' (2004) 23 *Computers and Security* 400, 405.

⁸⁸ For example, where material for one individual is entered into the file of another with a similar or identical name, notwithstanding a dissimilar address, such information then characterising the first with the second's record of bad debts or criminal record and so forth.

Table 3

Governments Agencies in Jordan connected to the e-government portal

No.	Government Agency	Stage I Emerging	Stage II Enhanced	Stage III Interactive	Stage IV Transactional	Stage V Connected	Availability of Privacy Policy/Statement	Website Address
1.	The Official Site of e-government	Yes	Yes	Yes	No	No	Yes	www.jordan.gov.jo
2.	Ministry of Finance	Yes	Yes	Yes	No	No	No	www.mof.gov.jo
3.	Ministry of Foreign Affairs	Yes	No	No	No	No	No	www.mfa.gov.jo
4.	Ministry of Health	Yes	Yes	No	No	No	No	www.moh.gov.jo
5.	Ministry of Higher Education and Scientific Research	Yes	Yes	Yes	No	No	No	www.mohe.gov.jo
6.	Ministry of Industry and Trade	Yes	Yes	Yes	No	No	No	www.mit.gov.jo
7.	Ministry of Information and Communications Technology	Yes	Yes	Yes	No	No	No	www.moict.gov.jo
8.	Ministry of Interior	Yes	Yes	No	No	No	No	www.moi.gov.jo
9.	Ministry of Labor	Yes	Yes	Yes	No	No	No	www.mol.gov.jo
10.	Ministry of Municipal Affairs	No	No	No	No	No	No	www.mma.gov.jo
11.	Ministry of Planning and International Cooperation	Yes	Yes	Yes	No	No	No	www.mop.gov.jo
12.	Ministry of Political Development	Yes	Yes	No	No	No	No	www.mopd.gov.jo
13.	Ministry of Public Sector Development	Yes	Yes	Yes	No	No	No	www.mopsd.gov.jo
14.	Ministry of Public Works and Housing	Yes	Yes	Yes	No	No	No	www.mpwh.gov.jo
15.	Ministry of Social Development	Yes	Yes	No	No	No	No	www.mosd.gov.jo
16.	Ministry of Transport	Yes	Yes	Yes	No	No	No	www.mot.gov.jo
17.	Amman Stock Exchange	Yes	Yes	Yes	No	No	No	www.exchange.jo
18.	Central Electricity Generating Co.	Yes	Yes	Yes	No	No	No	www.cegco.com.jo
19.	Central Bank of Jordan	Yes	Yes	Yes	No	No	No	www.cbj.gov.jo
20.	Civil Service Bureau	Yes	Yes	Yes	No	No	No	www.csb.gov.jo
21.	Department of Press and Publications	Yes	Yes	Yes	No	No	No	www.dpp.gov.jo
22.	Jordan Deposit Insurance Corporation	Yes	Yes	No	No	No	No	www.dic.gov.jo
23.	Development and Employment Fund	Yes	Yes	Yes	Yes	No	No	www.def.gov.jo
24.	Electricity Regulatory Commission	Yes	Yes	Yes	No	No	No	www.erc.gov.jo
25.	Executive Privatisation Commission	Yes	Yes	Yes	No	No	No	www.epc.gov.jo
26.	Jordan Chamber of Commerce	Yes	Yes	Yes	No	No	No	www.jocc.org.jo

26. Jordan Food and Drug Administration	Yes	Yes	Yes	No	No	No	www.jfda.jo
27. Orphans Fund Development Foundation	Yes	Yes	Yes	No	No	No	www.ofdc.gov.jo
28. Jordan Security Commission	Yes	Yes	Yes	No	No	No	www.jsc.gov.jo
29. National Information Technology Centre	Yes	Yes	Yes	No	No	No	www.nitc.gov.jo
30. Royal Jordanian	Yes	Yes	Yes	Yes	Yes	Yes	www.rj.com
31. Security Depository Centre	Yes	Yes	Yes	No	No	No	www.sdc.com.jo
32. Telecommunications Regulatory Commission	Yes	Yes	Yes	No	No	Yes	www.trc.gov.jo
33. Income and Sales Tax Department	Yes	Yes	Yes	No	No	No	www.incometax.gov.jo
34. Insurance Regulatory Commission	Yes	Yes	Yes	No	No	No	www.irc.gov.jo
35. Department of Lands and Survey	Yes	Yes	No	No	No	No	www.dls.gov.jo
36. Social Security Corporation	Yes	Yes	Yes	Yes	No	No	www.ssc.gov.jo
37. Department of Statistics	Yes	Yes	Yes	No	No	No	www.dos.gov.jo
38. Jordan Customs	Yes	Yes	Yes	Yes	No	No	www.customs.gov.jo
39. Civil Status and Passports Department	Yes	Yes	No	No	No	No	www.cspd.gov.jo
40. General Intelligence Department	Yes	Yes	Yes	No	No	No	www.gid.gov.jo

Table 4

Government Agencies Websites with Privacy Policies/Statements with FIPs (Jordan)

No	Agency	Availability of FIP Dimensions					Website Address
		Notice	Choice	Access	Security	Enforcement	
1.	The official site of e-government	Yes	Yes	Yes	No	No	www.jordan.gov.jo
2.	Telecommunications Regulatory Commission (TRC)	Yes	Yes	Yes	No	No	www.trc.gov.jo
3.	Royal Jordanian	Yes	Yes	Yes	Yes	No	www.rj.com

4.4.3 Privacy Impact Assessments (PIA) of the E-Government Initiative

The author believes that the above privacy concerns that have been identified in the case study of Jordan's e-government can be adequately addressed and explained if a privacy impact assessment had been conducted prior to the initiation of the e-government project. Stakeholders — such as government agencies, private institutions and individuals — will become concerned at the effects of these projects on individual privacy. The lack of such an assessment may lead to additional costs and burdens on these stakeholders if privacy concerns are addressed at later stages of project implementation. The lack of privacy impact assessment is another shortcoming in Jordan as it is difficult to provide adequate protection to individual's privacy when there is no privacy law or regulation (in this case, no requirement for such an assessment to be made). This section discusses privacy impact assessment and its importance in addressing privacy issues in the online environment.

Although the precise definition may vary from jurisdiction to jurisdiction, a privacy impact assessment (PIA) is defined by Blair Stewart as 'a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open to a proposal'. Another definition provided by Stewart of the PIA refers to it as 'an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated'.⁸⁹ To sum up, a

⁸⁹ Blair Stewart, *Privacy Impact Assessment* (1996) Privacy Law and Policy Reporter <<http://www.austlii.edu.au/au/journals/PLPR/1996/39.html>> at 1 July 2009.

PIA is an analysis of how personal information is collected, stored, shared, and managed in a government system.⁹⁰

PIAs are used to evaluate the privacy impact of computerisation or data collection projects proposed by government entities, in the same way that environmental impact assessments are used to identify and evaluate the environmental impact of projects such as dams or highways.⁹¹ A PIA provides a framework for identifying and addressing privacy issues. More specifically, it is an evaluation that is conducted to assess how the adoption of new information policies, the procurement of new computer systems, or the initiation of new data collection programs will affect individual privacy.⁹² However, PIA has not been used to evaluate the adoption, implementation and any other stages of the e-government project in Jordan. In other words, there was no assessment or measurement of how e-government in Jordan would impact on individual privacy.

The best example of the use of PIAs is the *US E-Government Act of 2002*.⁹³ The Act aims to improve the management and promotion of e-government services. It also allows US citizens to access to government's information and services. In addition, its provisions require that government agencies conduct privacy impact assessment in order to enhance the protection of personal information which has been collected by these agencies.

⁹⁰ United States Government Accountability Office, 'Privacy: Key Challenges', above n 55, 5.

⁹¹ James X Dempsey, Paige Anderson and Ari Schwartz, 'Privacy and E-Government: A Report to the United Nations Department of Economic and Social Affairs as background for the *World Public Sector Report: E-Government*' (Center for Democracy and Technology, 2003) 25.

⁹² *Ibid.*

⁹³ *E-Government Act of 2002*, 44 USC § 101, Pub L 107-347, 116 Stat 2899.

Accordingly, the *US E-Government Act of 2002* requires government agencies to conduct PIAs in the following circumstances: (1) ‘before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form’,⁹⁴ (2) before initiating any information collections of personal information using information technology methods.⁹⁵ In addition, the Act requires ‘agencies, if practicable, to make privacy impact assessments publicly available through agency websites, publication in the Federal Register, or any other means’.⁹⁶

It is believed that the level of privacy protection of personal information in the context of US e-government is largely adequate compared with the situation in Jordan. This is due to US e-government being based on the above mentioned Act. By contrast, Jordan’s e-government initiative is not established in accordance with such a law. Jordan’s e-government is nothing more than a national project seen by the policy makers in Jordan as catalyst for the country’s growth.

Furthermore, the implementation of PIAs increases the level of individual privacy in context of the US e-government. The PIA can achieve the following objectives: (1) ensure that handling information conforms to applicable legal, regulatory and policy requirements concerning privacy, (2) identify the risks and the impacts of collecting, maintaining and disclosing personal information in a government agency system, and (3) examine and

⁹⁴ Ibid sec 208(a)(i)

⁹⁵ Ibid sec 208(a)(ii).

⁹⁶ Ibid sec 208(b)(iii).

evaluate protections and alternative processes for treating personal information to avoid potential privacy concerns.⁹⁷

4.5 Concluding Remarks

Information and communications technology has been one of the fastest growing sectors in Jordan. The importance of ICT cannot be ignored, with ICT affecting all aspects of the Jordanian society, such as healthcare, education, employment, telecommunications, banking and commerce.

This chapter has examined the impacts of the ICT on individual privacy in the context of e-government of Jordan. The e-government in Jordan was implemented in order to deliver a variety of services to individuals across society irrespective of their location, economic status or education. Therefore, most government agencies provide services electronically.

However, in spite of the advantages of e-government, there has been a significant omission in its implementation in Jordan, namely the issue of individual privacy has never been addressed by the policy makers when they implemented the e-government program. The online study reported in this chapter identified the threats presented by the e-government to individual privacy. It revealed that most government agencies collect and use personal information without addressing the question of guidelines or policies to protect individual privacy.

⁹⁷ Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (2003) Office of Management and Budget <http://www.whitehouse.gov/omb/memoranda_m03-22/> at 30 December 2010.

Briefly, the rapid developments in ICT in Jordan have created many possible ways for government agencies to collect, store, access and process large amounts of personal information about its citizens. However, the success of e-government depends on the extent to which Jordanian feel they can trust government with the information they provide and receive in their online transactions. The risks involved are not due to these technological developments themselves, but rather to the lack of privacy legislation or guidelines that have as their main priority the spread of an awareness of issues related to privacy between individuals and government agencies and an adequate legislative and regulatory response.

Chapter Five

Privacy and Information and Communication Technology in Jordan: *The Private Sector*

5.1 Introduction

During the past few years, the Jordanian economy has been transformed. Economic reform in Jordan covered several areas, including the deregulation of business sectors, the privatisation of public services, and the elimination of trade barriers. These reforms may be interlocked. For example, the rapid development of ICTs made it necessary for the telecommunications sector in Jordan to become the first public enterprise to be privatised. Currently, this sector provides customers with variety of services and products that were unavailable to them before the start of privatisation process.

Further, the recent economic reform has made Jordan an active actor in the 'globalised' world. Jordan's accession to the World Trade Organisation (WTO) and signing of trade agreements with important partners including the US and the EU has signalled its broader participation. These agreements are strong factors in making Jordan's economy accessible to multinational institutions. Multinational and foreign companies are engaging in the Jordanian markets to provide customers with a range of products and services, particularly in the area of telecommunications and in the banking sector. Because of its international trade commitments, Jordan has introduced new laws and regulations to reform its ICT industry. The

significant laws adopted include: the *Telecommunications Law No 13 of 1995*,¹ the *Electronic Transactions Law No 85 of 2001*,² and the *Information Systems Crime Law No 30 of 2010*.³

While the reform of the ICT industry has many benefits, there are serious concerns about individual privacy, the lack of which (it is feared) may undermine these benefits. For example, as stated in the previous chapter, the government's 'Laptop for every University Student' initiative that aims to bridge the country's 'digital gap' by providing internet access and wireless technologies has extended its scope to include school students as young as 13 years of age. This has prompted growing fears regarding the issue of children's online privacy, given the lack of legal protection in this particular area too.

This chapter examines the issue of individual privacy in two important sectors in Jordan that were subject to reform and liberalisation: the telecommunications and the banking sectors. These two sectors were chosen for three reasons. Firstly, they are the most important sectors that have ability to collect, store, access and transfer large amounts of personal information. Secondly, many of the providers of telecommunications and banking services operating in Jordan are affiliates of foreign companies. The foreign entities may possess personal information of Jordanians and may

¹ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002* (Jordan), *Official Gazette*, No 4416, 17 February 2000. The original law was issued in the *Official Gazette*, No 4072, 1 October 1995.

² *Electronic Transaction Law No 85 of 2001* (Jordan), *Official Gazette*, No 4524, 31 December 2001, at 6010.

³ *Information Systems Crime Law No 30 of 2010* (Jordan) [*Arabic*] *Official Gazette*, No 5056, 16 September 2010, at 5334.

transfer the information to enterprises based outside Jordan. The enterprises based outside Jordan may misuse this information, and Jordanian jurisdiction may be lacking in regard to dealing with such practices when conducted 'off-shore'. Finally, the telecommunications and banking industries are currently heavily reliant on ICT channels to provide a variety of services and products to their customers. ICT channels, including text messages and internet banking, are widely used in Jordan. The use of text messages as a telemarketing tool has raised the issue of privacy invasion in Jordan.

The method adopted in this chapter to address individual privacy issues is based on an empirical analysis of the information privacy practices of the above mentioned sectors in Jordan. A study of these practices is undertaken to determine whether they provide adequate protection for individual privacy. To achieve this goal, the study relies on one source: the privacy 'policies' or 'statements' that are available on the websites of telecommunications companies and banks in Jordan. These privacy 'policies/statements' directly address a company's obligations and responsibilities regarding the protection of the personal information that the company obtains.

The chapter also provides two case studies in the chosen sectors in order to determine whether or not foreign companies adequately protect individual privacy in Jordan when engaging in cross-border transactions. The first part (below) provides an overview of economic reform in Jordan. The chapter

then goes on to examine Jordan's liberalisation program which has led Jordan to sign multilateral and bilateral trade agreements.

5.2 Economic and trade liberalisation in Jordan

Jordan's economic crises since the mid-to-late 1980s⁴ put Jordan under external pressure, particularly from the International Monetary Fund (IMF), to adopt an economic liberalisation program in 1989.⁵ In 1988, in order to deal with the crises, the Government of Jordan entered into a structural adjustment agreement with the IMF to restructure its debt payment schedule.⁶ In return, Jordan agreed to IMF demands for economic reform which included the removal of government subsidies, privatisation of public enterprises, cuts in state employment, and the gradual elimination of customs duties.⁷ The Government of Jordan regards privatisation as one of the centrepieces of its structural policy agenda.⁸ In 2000, in accordance with the *Privatisation Law No 25 of 2000*, it established the Executive Privatisation Commission (EPC) to study restructuring and privatisation of particular government agencies.⁹ As of 2009, the Government has completely achieved the privatisation of a number of public enterprises including: the Jordan Telecommunication Corporation (JTCC), the Jordan Electricity Authority

⁴ Karla J Cunningham, 'Factors Influencing Jordan's Information Revolution: Implications for Democracy' (2002) 56(2) *Middle East Journal* 240, 244.

⁵ Scott Greenwood, 'Jordan's "New Bargain": The Political Economy of Regime Security' (2003) 57(2) *Middle East Journal* 248, 260.

⁶ Steven E Lobell, 'The Second Face of American Security: The US-Jordan Free Trade Agreement as Security Policy' (2008) 27 *Comparative Strategy* 88, 91.

⁷ Anne Marie Baylouny, 'Military Welfare: Neo-liberalism and Jordanian Policy' (2008) 62(2) *Middle East Journal* 277, 292.

⁸ Michel Marto and Ziad Fariz, *Jordan Letter of Intent and Memorandum on Economic and Financial Policies for 2000* (2000) International Monetary Fund <<http://www.imf.org/external/np/loi/2000/jor/01/index.htm>> at 9 July 2009.

⁹ *Privatization Law No 25 of 2000* (Jordan), <<http://www.epc.gov.jo/EPC/Home/PrivateLaw/tabid/86/Default.aspx>> at 9 July 2009.

(JEA), the Irbid District Electricity Company (IDECO), the Jordan Electric Power Company (JEPCO), the Aqaba Railway Corporation (ARC), the Jordan Cement Factories Company (JEFC), the Public Transport Corporation (PTC) and the Arab Potash Company (APC).

By far one of the most successful privatised public enterprises in Jordan is the transformation of the telecommunications sector from a government-owned JTC alone to a sector with multiple competing corporate entities. Jordan was the first country in the Arab world to have fully liberalised this sector and has updated 75 per cent of its ICT related laws, improving the business environment for local and international investors.¹⁰ JTC itself is now privately owned and operates in competition with a number of new providers.

In respect to foreign investments in Jordan, the *Investment Promotion Law No 16 of 1995* was passed offering financial incentives to attract local and foreign investment to Jordan.¹¹ The law provides equal treatment of domestic and foreign investors. Article 24 of the law stipulates that non-Jordanian investors in any projects governed by the law should be afforded the same treatment as Jordanian nationals, with the exception of certain sectors involving national security and military activities. The law guarantees foreign investors the transfer of profits and repatriation of the foreign capital

¹⁰ Jordan Investment Board, *Vital Sectors: ICT Sector* (2009) Jordan Investment Board <http://www.theodora.com/wfbcurent/jordan/jordan_communications.html> at 10 July 2009.

¹¹ *Investment Promotion Law No 16 of 1995* (Jordan), *Official Gazette*, No 4075, 16 October 1996 and amended in the *Law No 13 of 2000* (Jordan) *Official Gazette*, No 4423, 2 April 2000. Text avail: <<http://www.jordaninvestment.com>>.

invested.¹² Total investments in the projects promoted under this law were USD 3131.9 million in 2007, representing an increase from the figure of USD 1118.5 million in 2000. Foreign investment represented 47 per cent of total investment in 2007.¹³

The strategy of the liberalisation program in Jordan relies on two main factors: first, Jordan gaining membership of major international economic organisations (in particular the WTO); second, Jordan signing bilateral trade agreements with its strategic trade partners the United States and the European Union (EU).¹⁴ The following sections examine these factors that have delivered many regulatory changes and amendments in Jordan, and discuss whether or not these factors have had impacts on Jordan's privacy regulatory environment, particularly in the ICT sector.

5.2.1 Jordan and the World Trade Organisation (WTO)

In January 1994, Jordan submitted an application for accession to the *General Agreement on Tariffs and Trade* (GATT), which became an application for membership of the WTO after the establishment of the WTO in January 1995 as a result of the Uruguay Round of trade negotiations.¹⁵ The Working Party reviewing Jordan's application raised several concerns regarding the country's economic structure, monetary and fiscal policies, and import and

¹² Ibid art 5(c).

¹³ World Trade Organisation, 'Trade Policy Review of Jordan: Report by the Secretariat' (World Trade Organisation, 2008) 17. For the most recent figures, see United Nations Conference on Trade and Development (UNCTAD), *World Investment Report 2010. Investing in a Low Carbon Economy* (2010) <http://www.unctad.org/sections/dite_dir/docs/wir10_fs_jo_en.pdf> at 2 January 2011.

¹⁴ Cunningham, above n 4, 251.

¹⁵ On 23 December 1999, a decision was made by the WTO General Council that Jordan may accede to the WTO and Jordan became the 136th member. See World Trade Organisation, 'Accession of the Hashemite Kingdom of Jordan' WTO Doc WT/ACC/JOR/34 (23 December 1999) (Decision on 17 December 1999) avail <www.wto.org> at 2 January 2011.

export regulations.¹⁶ To address these concerns, Jordan decided to reform its economic sectors, particularly trade regulations to conform to WTO obligations. The telecommunications and banking sectors were subject to intensive reform by Jordan's government to meet the following obligations.

5.2.1.1 Jordan's obligations in Telecommunications under WTO GATS

In the telecommunications sector, Jordan incurred significant trade liberalisation and competition obligations under the *General Agreement on Trade in Services* (GATS), in relation to both basic and value added services. Under its general GATS obligations, Jordan is obliged to extend most favoured nation (MFN) status to other WTO member countries and 'ensure transparency of local' regulations.¹⁷ Those obligations and more specific ones spelt out in under the *WTO Basic Telecommunications Agreement* (the relevant sector specific agreement) involve basic telecommunications service provision (including voice telephone services, telegraph services, facsimile services, private leased circuit services, packet-switched data transmission services (internet), and circuit-switched data transmission services); and value added service provision (including e-mail, voice mail, online information and data base-retrieval, electronic data interchange and code and protocol

¹⁶ World Trade Organisation, 'Report of the Working Party on the Accession of the Hashemite Kingdom of Jordan to the World Trade Organisation' (1999) WTO Doc WT/ACC/JOR/33 WT/MIN (99)/9 (3 December 1999) <<http://docsonline.wto.org/DDFDocuments/t/WT/ACC/JOR33.DOC>> at 10 July 2009.

¹⁷ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), art II, Annex IB, 286, <http://www.wto.org/english/docs_e/legal_e/26-gats.pdf>. See also World Trade Organisation, 'Trade Policy Review - Jordan' (2008) Paper No WT/TPR/S/206, 121 (Table AIV.2) 6 October 2008. See also 'Info Dev/ITU, *ICT Regulations Toolkit* <<http://www.ictregulationtoolkit.org/en/section.1651.html>> at 31 January 2011.

conversion).¹⁸ Jordan was obliged to terminate the state's monopoly over telecommunications, with the exclusive rights of the Jordan Telecommunications Company (JTC) to be withdrawn by 2004.¹⁹ Also to be considered were the prevention of anti-competitive practices in the sector, and security of regulatory independence.²⁰

Further, Jordan is committed to meet the obligations included in the 1996 Reference Paper for the WTO Agreement on Basic Telecommunications Services that was later integrated into GATS.²¹ Therefore, Jordan must:

1. Implement laws and regulations to prevent major suppliers from engaging in anti-competitive practices in telecommunications (for example, engaging in anti-competitive cross-subsidisation, and the use sensitive information from competitors with anti-competitive results).
2. Administer universal service obligations (USO) in a transparent, non-discriminatory, and competitively neutral manner. The 1996 Reference Paper specifies that USOs will not be regarded as anticompetitive per se.
3. Ensure public liability of licensing criteria.

¹⁸ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), art XX, Annex IB, 299. See also World Trade Organisation, 'Report of the Working Party on the Accession of Jordan to the World Trade Organisation: Trade in Services: Schedule of Specific Commitments on Services' (World Trade Organisation, 1999) WTO Doc WT.ACC/JOR/33/Add.2, 15 December 2000, 14-15 <http://www.mit.gov.jo/Portals/0/wot/services_schedule.pdf> at 10 January 2011.

¹⁹ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), art VIII (4), Annex IB, 291. See also World Trade Organisation: Trade in Services: Schedule of Specific Commitments on Services', Sector-Specific Commitments: Telecommunications Services, Doc No GATS/SC/128, 15 December 2000.

²⁰ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), art IX, Annex IB, 292. See also Cunningham, above n 4, 253.

²¹ World Trade Organisation, *Reference Paper: Negotiating Group on Basic Telecommunications* (24 April 1996) WTO <http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm> at 23 January 2011. See WTO Doc GATS/SC/128, 15 December 2000. The WTO *Agreement on Basic Telecommunications Services* was integrated into the WTO GATS as the Fourth Protocol to GATS, adopted 15 April 1997 (entered into force 8 February 1998).

4. Establish an independent regulator to monitor the telecommunications market. The regulatory body could be a government ministry or an independent commission with the power to issue decisions, instructions and procedures which must be impartial with regard to telecommunications actors.
5. Allocate and use of scarce resources, which may include: radio spectrum, numbers and rights of way. This must be carried out in an objective, timely, transparent and non-discriminatory manner.

Jordan's commitments to the above in the telecommunications sector entail a number of legal obligations in regard to: (1) market access, (2) foreign ownership and national treatment, (3) anti-competitive laws and regulations, (4) establishment of an independent regulator; (5) market liberalisation; and finally, (6) measures enacted in order to effect such commitments.²²

As a result, Jordan's government made the first move towards the liberalisation of telecommunications sector by enacting the *Telecommunications Law No 13 of 1995*.²³ The law has ended state monopoly of the above services. The legislation was designed to create a fair and competitive regulatory framework, to address the issuance of licences, to separate regulatory and operating sectors, and to facilitate the privatisation process. The law has established the Telecommunications Regulatory Commission (TRC), Jordan's national telecommunications authority,²⁴ which

²² Kent Bressie, Michael Kende and Howard Williams, 'Telecommunications Trade Liberalisation and the WTO' (2005) 7(2) *Info* 3, 9.

²³ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002* (Jordan).

²⁴ Cunningham, above n 4, 242.

has the responsibility to implement Jordan's obligations in accordance with GATS. (The role of the TRC is discussed in a separate section, further below).

5.2.1.2 Jordan's obligations in the banking sector under WTO GATS

The banking sector in Jordan is an important part of the Jordanian economy. The sector is a large employer and provides working opportunities for the country's educated workforce. The sector also includes financial services providers who provide investment and financial market services.²⁵ The estimated assets of this sector rose by JOD 18.3 billion (JOD 1 = USD 0.72) to JOD 31.2 billion, an increase of 141.9 per cent, between the year 2000 and 2009.²⁶

Jordan made significant GATS commitments in the banking sector.²⁷ One of the most significant commitments is the permission for full ownership of banks by foreign persons or entities.²⁸ Jordan adopts the four modes of supply concerning financial services commitments.²⁹ Consequently, there are no restrictions on foreign investors or entities that wish to establish

²⁵ Ministry of Industry and Trade, 'Assessment of Trade in Services of the Hashemite Kingdom of Jordan: A Project of the Ministry of Industry and Trade (MoIT) and United Nations Conference on Trade and Development (UNCTAD)' (2006) pt II, 64.

²⁶ Association of Banks in Jordan, 'Development of the Jordanian Banking Sector (2000-2009)' (Association of Banks in Jordan 2010) 27.

²⁷ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), art XIX, pt IV, Annex IB, 298.

²⁸ World Trade Organisation, 'Trade Policy Review-Jordan' (2008) Paper No WT/TPR/S/206, 115, (Table AIV.3) 6 October 2008. See services identified in the Services Sectoral Classification List in WTO Doc No S/L/92, 28 March 2001.

²⁹ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), art I, pt I, Annex IB, 285. The four modes of supply are: Mode 1 -Cross border trade: from the territory of one Member into the territory of any other member, Mode 2 - Consumption abroad: in the territory of one Member to the service consumer of any other Member, Mode 3 - Commercial presence: by a service supplier of one Member, through commercial presence, in territory of any other Member, and Mode 4 - Presence of natural person: by a service supplier one Member, through the presence of natural persons of a Member in the territory of any other Member.

branches or subsidiaries in the banking sector. Jordanian law treats local and foreign banks equally.³⁰ Therefore, transactions by foreign banks operating in Jordan are not restricted or controlled in any way other than are domestic operators. Their services include: acceptance of deposits and other repayable funds from the public, lending services including: consumer credit, factoring, mortgage credit, and financing and commercial transactions, financial leasing and all payment and money transmission services.³¹

Although the banking sector in Jordan is 'heavily regulated' in terms of the level of statutory controls and disciplines as well as regulatory compliance and oversight standards, it does not suffer from barriers or restrictions. The regulations of this sector are concerned with licensing, registration and certification standards.³²

A number of laws were enacted to meet WTO obligations in the banking sector including: the *Investment Promotion Law No 16 of 1995* providing non-discriminatory treatment of foreign investors,³³ the *Banking Law No 28 of 2008* that grants the Central Bank of Jordan the authority to issue licences

³⁰ World Trade Organisation, 'Trade in Services: The Hashemite Kingdom of Jordan; Schedule of Specific Commitments' (World Trade Organisation, 2000) WTO Doc No GATS/SC/128, 15 December 2000, available at <www.wto.org>.

³¹ World Trade Organisation, 'Report of the Working Party on the Accession of Jordan to the World Trade Organisation: Trade in Services: Schedule of Specific Commitments on Services' (World Trade Organisation, 1999) WTO Doc No WT.ACC/JOR/33/Add.2, 22. For text, see <http://www.mit.gov.jo/Portals/0/wot/services_schedule.pdf>.

³² Ministry of Industry and Trade, 'Assessment of Trade in Services of the Hashemite Kingdom of Jordan', above n 25, pt II, 83.

³³ *Investment Promotion Law No 16 of 1995* (Jordan).

for new banks,³⁴ and the *Electronic Transactions Law No 85 of 2001* to address issues related to electronic commerce and electronic banking.³⁵

Furthermore, apart from WTO GATS commitments, Jordan commenced the amendment of existing laws and enactment of laws in various areas. In the area of intellectual property rights, amendments were made to the trademarks and copyrights legislation, and new laws on patents, models and industrial design, integrated circuits, trade secrets and unfair competition were introduced. In other areas, laws were also enacted to replace existing laws that were not in conformity with the WTO requirements such as the Customs Law and General Sales Tax Law. New regulations on the safeguard of national production, non-Jordanian investments, and consular fees were also enacted.³⁶

The author believes that during the undertaking of those regulatory changes in relation to Jordan's obligations under GATS regarding the telecommunications and banking sectors, the issue of privacy for this sector was not considered. It appears that most of the laws that have been introduced to meet GATS obligations are intended to attract foreign investment, and facilitate greater market access in order to address Jordan's economic crisis that occurred in 1989, regardless of whether or not these obligations may have an impact on individual privacy. For example, under Jordan's commitments to the WTO, if a financial service supplier in WTO

³⁴ *Banking Law No 28 of 2000* (Jordan) *Official Gazette*, No 4448, 1 August 2000, 2950.

³⁵ *Electronic Transaction Law No 85 of 2001* (Jordan).

³⁶ Jordan Economic & Commerce Bureau, *Jordan & the WTO* (2005) Embassy of Jordan, Washington, DC <http://www.jordanecb.org/agreements_jowto.shtml> at 10 July 2009.

member state (for example, China)³⁷ seeks to provide banking services through electronic means such as automated teller machines (ATMs) in Jordan, then because Jordan has committed to not restricting cross-border supply, Jordan must ensure that the financial service supplier in China has full access, and use of public telecommunications networks to be able to provide ATM services in Jordan. One privacy concern that arises from this is that personal information about Jordanians stored on the ATM card may be accessed and transferred to China as a WTO member.

The author's view is that Jordan should introduce a privacy protection law so that Article XIV of the GATS can be enforced. As a general exception and provided that such measures can be interpreted as constituting an 'arbitrary or unjustifiable discrimination between countries where like conditions prevail or a disguised restriction on trade in services', this Article provides that nothing in the GATS Agreements can be interpreted to prevent the adoption of laws and/or regulations that are necessary to protect 'the privacy of individuals in relation to the processing of personal information and the protection of confidentiality of personal records and accounts'.³⁸ Unless otherwise, a privacy protection law and/or regulations in place, Jordan cannot rely on this exception not to comply with its commitments under the GATS provisions based on the argument that complying with such commitments may violate individual privacy.

³⁷ China became a WTO member on 10 November 2001, see World Trade Organisation, *WTO News: WTO Successfully Concludes Negotiations on China's Entry* (2001) WTO <http://www.wto.org/english/news_e/pres01_e/pr243_e.htm> at 23 January 2011.

³⁸ World Trade Organisation, 'General Agreement on Trade in Services' (GATS), Annex 1B, pt 2, art XIV(c)(ii), 295.

In addition to WTO obligations, Jordan has entered into a number of regional and international trade agreements in order to strengthen its economy. This has involved a number of ICTs. For example, on a regional level, Jordan and Israel signed an agreement in September 1999 on installing a fibre-optic cable linking the two countries. Jordan also joined Fiberoptic Link Around the Globe (FLAG) in July 1999, which is a trans-global largely undersea cable that passes through Japan, the US, the Middle East and Britain. The network equips Jordan with high-speed internet access to enable it to deliver e-government services to businesses and citizens. There is a great possibility that in the near future the private sector will be able to use this network.

On an international level, Jordan's trade agreements with important trade partners (the US and EU) have imposed further obligations on Jordan to liberalise the ICT industry. The next section examines these trade agreements.

5.2.2 The Jordan-US Free Trade Agreement (JUSFTA)³⁹

On 24 October 2000, the Hashemite Kingdom of Jordan and the United States signed the Jordan-US Free Trade Agreement (JUSTFA), which entered into force on 17 December 2001. Jordan was the first Arab country to sign a free trade agreement with the US. The agreement led Jordan to sign similar trade agreements with other countries including: the States of

³⁹ *Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Agreement* (2000) <http://www.mit.gov.jo/Portals/0/TextOA/AGREEMENT_TEXT.pdf> at 10 March 2010.

the European Free Trade Association (EFTA) in 2001,⁴⁰ Singapore in 2004,⁴¹ as well as Canada,⁴² and Turkey,⁴³ (both in 2009). Due to the special Jordan-US relationship from economic and political perspectives, the focus of this section will concentrate solely on the JUSFTA.

The JUSFTA reflects the demands made by the US for economic and political reforms in Jordan. The US saw the agreement as a condition imposed on Jordan to sign a peace treaty with Israel in 1994, and, by supporting Jordan's economic reform, as providing greater economic growth and stability in the Middle East. The United States' decision to sign an FTA with Jordan was also heavily influenced by Jordan's accession to the WTO in 1999.⁴⁴

By 2005, the United States was Jordan's largest export market and fourth largest source of imports. The total bilateral trade between the countries had increased by 17.7 per cent from 2004, reaching USD 1.90 billion. For the same period, Jordan's exports to the US increased by 15.90 per cent, compared to 10.30 per cent increase in Jordan's export to the world.⁴⁵ The

⁴⁰ *Agreement between the EFTA States and the Hashemite Kingdom of Jordan*, signed 21 June 2001 (entered into force 1 September 2002. EFTA States include: Iceland, Liechtenstein, Norway, and Switzerland. For text, see <<http://www.mit.gov.jo/Portals/0/efta/EFTA.pdf>> at 12 February 2011.

⁴¹ *Agreement between the Government of the Hashemite Kingdom of Jordan and the Government of Singapore on the Establishment of a Free Trade Area*, signed 16 May 2004 (entered into force 22 August 2005). For text, see <http://www.mit.gov.jo/Portals/0/Jordan_20Singapore_20FTA.pdf> at 12 February 2011.

⁴² *Free Trade Agreement between the Hashemite Kingdom of Jordan and Canada*, signed 28 June 2009. Text avail <<http://www.mit.gov.jo>> at 12 February 2011.

⁴³ *Association Agreement Establishing a Free Trade Area between the Hashemite Kingdom of Jordan and the Republic of Turkey*, signed 1 December 2009 (entered into force 1 March 2011. For text, see <<http://www.mit.gov.jo/portals/0/JO%20EN%20Agreement%20Text.pdf>> at 12 February 2011.

⁴⁴ Cunningham, above n 4, 252.

⁴⁵ James Cassing and Anna Maria Salameh, 'Jordan - United States Free Trade Agreement Economic Impact Study: Searching for Effects of the FTA on Exports, Imports and Trade Related Investments' (United States Agency for International Development (USAID, 2006) 19.

US remains Jordan's largest export market and is now the nation's third largest source of imports.⁴⁶ It was expected that the FTA would speed Jordan's economic growth, allowing for the possibility that it would become less dependent on foreign aid.⁴⁷ While economic growth has occurred, Jordan still relies heavily on foreign aid, particularly from the US and remains that country's fourth largest recipient of aid.⁴⁸ Politically, the US saw the FTA as a reward for Jordan for its support for the 'war on terrorism', with such support including intelligence sharing, allowing the US military to use Jordan's military bases, and for US airplanes to use Jordanian airspace.⁴⁹

The FTA will eventually eliminate tariffs and non-tariff barriers for goods and services originating in both countries. The FTA also contains — for the first time ever in the text of a trade agreement — provisions addressing new issues such as trade and environment,⁵⁰ trade and labour,⁵¹ and electronic commerce.⁵² In addition, provisions addressing intellectual property rights protection,⁵³ balance of payments,⁵⁴ rules of origin,⁵⁵ safeguards (regarding

⁴⁶ Exports to the US comprise 17.3% of all exports; imports from the US comprise 6.94% (2009) of all imports: CIA, *World Factbook* <<https://www.cia.gov/library/publications/the-world-factbook/geos/jo.html#Econ>> at 1 February 2011.

⁴⁷ Bashar H Malkawi, 'E-Commerce in Light of International Trade Agreements: The WTO and the United States-Jordan Free Trade Agreement' (2006) 10 *International Journal of Law and Information Technology* 1, 7.

⁴⁸ Department of Commerce, *U.S.-Jordan Free Trade Agreement (FTA)* (2009) US Commercial Service <<http://www.buyusa.gov/jordan/en/fta.html>> at 28 August 2009.

⁴⁹ Lobell, above n 6, 95.

⁵⁰ *Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Agreement* (2000) <http://www.mit.gov.jo/Portals/0/TextOA/AGREEMENT_TEXT.pdf>.

⁵¹ *Ibid* art 6.

⁵² *Ibid* art 7.

⁵³ *Ibid* art 4.

⁵⁴ *Ibid* art 11.

⁵⁵ *Ibid* art 14.

reduction or elimination of duties (not privacy safeguards),⁵⁶ and procedural matters are also found in JUSFTA.⁵⁷

However, the most relevant ICT provisions in this agreement are those mentioned in Article 7 which covers specifically, electronic commerce.

Article 7 provides:

1. Recognising the economic growth and opportunity provided by electronic commerce and the importance of avoiding barriers to its use and development, each Party shall seek to refrain from:
 - (a) deviating from its existing practice of not imposing customs duties on electronic transmissions;
 - (b) imposing unnecessary barriers on electronic transmissions, including digitised products; and.....
2. The Parties shall also make publicly available all relevant laws, regulations, and requirements affecting electronic commerce.
3. The Parties reaffirm the principles announced in the US-Jordan Joint Statement on Electronic Commerce.

With respect to personal information protection, a number of comments can be made in relation to the above provisions. First, article 7(1) sheds light on the economic benefits and opportunities that may result from the e-commerce and related technologies for both parties. However, these benefits and opportunities may not be achieved for Jordan which does not have laws to regulate information practices in this type of business. By contrast, the US legal system (as it will be discussed in Chapter Seven) has a number of laws and/or regulations to protect personal information in the context of e-commerce.

⁵⁶ Ibid art 10.

⁵⁷ Ibid arts 16, 17.

Second, this article requires that both parties allow the exchange of information through electronic means without any limitations. However, the article did not suggest what policy that can be implemented to protect the exchanged information. It should have expressly stressed the importance of protecting personal information for successful e-commerce.

Third, article 7(2) recommends that both parties make necessary regulatory changes affecting e-commerce. One interpretation of this article is that it may mean that, neither party should introduce laws and regulations that may become obstacles to the growth of e-commerce. As introducing comprehensive privacy legislation to protect personal information may negatively affect the growth of e-commerce, such legislation would be not merely inadvisable, it would be contrary to the agreement. This interpretation is supported by the principles included in the US-Jordan Joint Statements on E-commerce⁵⁸ where both parties agreed on the following principles (among others and numbered below for convenience):

1. The private sector (not government) is envisaged as leading ‘the development of electronic commerce and establishing business practice’.
2. Both parties should refrain from ‘imposing unnecessary regulations or restrictions on electronic commerce. Government actions, when needed, ‘should be transparent, minimal, non-discriminatory and predictable to the private sector’.

⁵⁸ *U.S.-Jordan Joint Statement on Electronic Commerce*
<http://www.jordanusfta.com/documents/joint_statement_on_e-commerce.pdf> at 28 August 2009.

3. Governments are to encourage effective self-regulation through measures including codes of conduct, model contracts, guidelines and enforcement mechanisms to be developed by the private sector.
4. International cooperation is seen as necessary to assist the creation of ‘a seamless environment for electronic commerce’.⁵⁹

Both parties encouraged all countries to open their markets without restrictions to local and foreign investments in ICT infrastructure to help modernise ICT infrastructure. Both parties state they are ready to advance international cooperation and to avail themselves of international organisations and financial institutions to achieve this goal. Competition in information and communications markets is to be promoted to expedite the cost-effective uptake of technology that is necessary for growth of opportunity and economic progress.

Further, both parties will cooperate in (1) using the internet to address social challenges (for example, provide new skilling for working adults); (2) increasing access to health care (such as in isolated areas); (3) improving the quality of life of people with disabilities; and (4) strengthening democracy.⁶⁰ Universal access to technological literacy is seen as desirable. Here and in relation to ensuring rural area access, government is seen to have an important role to play.

⁵⁹ Note the principles in the *U.S.-Jordan Joint Statement on Electronic Commerce* (above n 58) are numbered for the convenience of the reader (not numbered in original document).

⁶⁰ *U.S.-Jordan Joint Statement on Electronic Commerce* <http://www.jordanusfta.com/documents/joint_statement_on_e-commerce.pdf> at 28 August 2009.

With regards to information, both parties agreed that electronic transmissions (information, contents) should be transmitted freely across national borders. Revealingly, both parties appear to limit the development of any barrier to the trade, agreeing that ‘trade barriers to the free flow of contents do not exist today and should not be created in the future’.⁶¹ The US strongly supports the free flow of information and regards privacy or data protection laws as establishing non-tariff trade barriers that protect national industries and communications providers.⁶² The ‘free flow’ concept is regarded as fundamentally important to US businesses. As one author states:

The very idea that a simple transfer of information between a parent and its affiliates can be subject to restrictions seems unthinkable to U.S. executives, most of whom have grown up in a society where information has always flowed freely across thousands of miles.⁶³

As for privacy of personal information, both governments agreed that effective privacy protection is necessary as is the continuous free flow of information. Consumers’ privacy concerns should be considered by governments and businesses with the role of the former seen as ‘encouraging the private sector to develop and implement enforcement mechanisms including guidelines and ... verification and recourse methodologies’. The privacy protection policy was to be flexible as each industry has a different

⁶¹ However, the document also notes that consumers should be empowered by access to filtering devices to block content they do not wish themselves (or perhaps their children) to receive. However this ‘blocking’ is at the consumer not government or regulator level. *U.S.-Jordan Joint Statement on Electronic Commerce* <http://www.jordanusfta.com/documents/joint_statement_on_e-commerce.pdf> at 28 August 2009 .

⁶² Pricilla M Regan, 'The Globalization of Privacy: Implications of Recent Changes in Europe' (1993) 52(3) *American Journal of Economics and Sociology* 257, 260.

⁶³ Martin D J Buss, 'Legislative Threat to Transborder Data Flow' (1984) 62(3) *Harvard Business Review* 111, 112.

method of collection of information, and the usage and contents of that information also varied.⁶⁴

For both parties consumer protection is important in the online environment. They agreed to take all necessary actions to enforce existing consumer protection laws, enacting new laws, if required, providing consumer education, and industry supported mechanisms ‘to empower consumers and resolve consumer complaints and concerns’.⁶⁵

Commenting on the above, the author argues that the US has used its trade agreement with Jordan to transform Jordan into a follower or supporting country, rather than a trade partner. The intention of JUSFTA was to empower certain pro-Western actors in Jordan (including the king and his cabinet, military personnel, and top bureaucrats) and to strengthen private businesses which have benefited from trading with companies in US and Europe (for example, government spending on defence contracts, and capital intensive projects).⁶⁶ This eventually will weaken Jordanian opponents to US policies (such as nationalists and anti-globalisation groups).

Further, it is believed that the US wishes to use the free trade agreement with Jordan to encourage Jordan to adopt certain policies that meet US national interests. Jordan is viewed by the US as an important ally in the war on terrorism and an influential peacemaking partner in the Middle East

⁶⁴ The OECD Privacy Protection Guidelines were held up as an ‘appropriate basis’ for policy development: *U.S.-Jordan Joint Statement on Electronic Commerce* <http://www.jordanusfta.com/documents/joint_statement_on_e-commerce.pdf> at 28 August 2009.

⁶⁵ Ibid.

⁶⁶ Lobell, above n 6, 92.

peace process. It is also believed that Jordan's unwillingness to legislate privacy protection law is at least in part motivated by a desire to increase US companies' investments in Jordan. It is feared that any attempt to legislate for privacy protection in Jordan may result in a turn down in the number US companies desiring to operate in Jordan or in the extent of their operations. Several US companies (including Sun Micro systems, Oracle Corporation, Intel, and Microsoft) are committed to providing training and other initiatives to Jordan in the ICT sector.⁶⁷

The US influence on Jordan's domestic policy clearly appears in Jordan's adoption of the above second and third principles in its Statement of Government Policy for year 2007 on the ICT and Postal Service in Jordan. Provisions included in paragraph 73 of this Statement are, to a large extent, similar to those expressed the general principles included in the US-Jordan Joint Statement on E-commerce. It clearly provides that, with the exception of internet, the Government believes that self-regulation is the most appropriate approach to be adopted to address ICT.⁶⁸ It also states that Jordan's ICT market should be opened to private investments and that no restrictive regulations are to be introduced to the ICT sector in Jordan.⁶⁹ Furthermore, US policy's influence is also noticeable in the Jordan's *Telecommunications Law No 13 of 1995*. Article 6 assigns several duties and responsibilities to be undertaken by the TRC. One responsibility assigned to

⁶⁷ ESIS, *Regulatory Developments in Jordan - Master Report: Jordan Efforts to Play a Key Role in the Regional IT Market* (2000) ESIS <<http://www.eu-esis.org/esis2reg/JOreg4.htm>> at 6 January 2011.

⁶⁸ Government of Jordan, 'Statement of Government Policy 2007 on the Information & Communications Technology & Postal Sectors' (Ministry of Information & Communications Technology, 2007) para 73, 19–20, <http://trc.gov.jo/images/stories/pdf/ICT_Policy_2007.pdf?lang=english> at 20 December 2010.

⁶⁹ Ibid para 86, 22.

the TRC is to encourage the adoption of a self-regulation regime by the ICT sectors in Jordan.⁷⁰

However, with respect to the term ‘effective self-regulation’ included in the US-Jordan Joint Statement on E-commerce, two questions arise. First: How is the term ‘effective’ to be defined? Indeed, how can effectiveness be measured when there is no standard benchmark implemented in Jordan against which to measure suggested guidelines and code of conducts? It will be almost impossible to measure the effectiveness of any guidelines or codes of conduct due to the absence of any laws, regulations or standard benchmarks for privacy protection in Jordan. Second: if ‘self-regulation’ to be adopted through guidelines and/or codes of conduct in Jordan, who is to enforce these guidelines and codes of conduct? These two questions are subject to further examinations in the coming sections.

5.2.3 The Jordan-European Association Agreement⁷¹

Jordan and the EU signed an association agreement on 24 November 1997 which entered into force on 1 May 2002, superseding the Jordan-EU Economic Cooperation Agreement of 1977. The Association Agreement (AA) aims to create a free trade area between EU and Jordan over a 12 year timeframe, in conformity with WTO rules. It also establishes a comprehensive framework for political, economic, trade and financial

⁷⁰ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002* (Jordan) art 6(g).

⁷¹ EURO-Mediterranean Agreement: Establishing an Association between the European Communities and their Member States, of the One Part, and the Hashemite Kingdom of Jordan, of the Other Part, OJ L129/3, Vol 45, 15 May 2002, <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:129:0003:0165:EN:PDF>>.

investment, social, and cultural cooperation.⁷² In this context, unlike other trade agreements signed by Jordan (for trade liberalisation), the AA goes further by aiming to achieve sustainable social and political developments that will affect people's lives in Jordan.⁷³ The Agreement includes three major components of cooperation:

1. Political cooperation

Both parties agreed to strengthen their political relations to develop a common understanding on international issues that may have substantial effects on either party. This component aims to enhance peace, security, human rights, democracy and regional stability and development.⁷⁴

2. Economic and financial cooperation

Both parties agreed to gradually establish a free trade area by the year 2014. The free trade agreement is based on the AA and in accordance with provisions included in the WTO General Agreement on Tariffs and Trade (GATT) of 1994.⁷⁵ The AA includes provisions on trade in industrial and agricultural products,⁷⁶ right of establishment and services,⁷⁷ cross-border supply of services,⁷⁸ payments and capital movements,⁷⁹ competition, intellectual property rights,⁸⁰ economic cooperation in the fields of education

⁷² Ibid art 1(2).

⁷³ Mohammad Nabulsi, 'Implementation of Jordan-EU Action Plan: A CSS Independent Evaluation' (Centre for Strategic Studies 2009) 1.

⁷⁴ EURO-Mediterranean Agreement [2002] OJ L 129/3, arts 3, 4.

⁷⁵ Ibid art 6

⁷⁶ Ibid arts 7–29.

⁷⁷ Ibid arts 30–36.

⁷⁸ Ibid arts 37–47.

⁷⁹ Ibid arts 48–52.

⁸⁰ Ibid arts 53–58.

and training,⁸¹ science and technology,⁸² financial services,⁸³ information infrastructure and telecommunications,⁸⁴ money laundering,⁸⁵ and the fight against illegal drugs.⁸⁶

3. Social and cultural cooperation

This component aims to address social and cultural issues related to both parties. Both parties agreed to find ways to address issues such as: migrant communities' living and working conditions, migration, and illegal immigration. In addition, they agreed on projects and programs that provide training on equality of treatment for citizens of both parties, on awareness of cultures and civilisations, on tolerance and on the elimination of discrimination.⁸⁷

With respect to social development, both parties agreed to take immediate actions to create jobs in order to reduce the number of illegal immigrants; to promote the role of women in social and economic development through education, the development of Jordanian family planning and mother and child protection programs; to improve the social security system, and the healthcare system; and to improve living conditions for disadvantaged areas.⁸⁸

⁸¹ Ibid art 63.

⁸² Ibid art 64.

⁸³ Ibid art 70.

⁸⁴ Ibid art 73.

⁸⁵ Ibid art 78.

⁸⁶ Ibid art 79.

⁸⁷ Ibid art 80.

⁸⁸ Ibid art 82.

The parties have also acknowledged the importance of developing mutual cultural respect in the provisions included in the AA. In this context, both parties agreed when identifying joint training and cooperative projects and programs to place particular emphasis on young people, on self-expression and communication skills using both written and audio-visual media as well as on heritage conservation issues and the dissemination of culture.⁸⁹

For Jordan to maximise benefits from the AA, Jordan must meet a number of obligations set out in the so-called the 'Action Plan'. The importance of the Action Plan is that it may lead to the development of new contractual relations with EU member states, if the EU is satisfied with Jordan's progress on these obligations. Further, implementing action plan obligations by Jordan is a condition to the establishment of a free trade area with the EU by 2014 in accordance with WTO rules. The following section discusses the role of the EU-Jordan Action Plan in Jordan's political, economic and political reform.

5.2.3.1 EU-Jordan Action Plan

The Action Plan was adopted in January 2005 with a timeframe of from three to five years. It aims to help Jordan fulfil the terms of the AA and support Jordan's political, economic and social reform objectives. It assigns Jordan a set of priorities in areas within the scope of the AA. Among these priorities, all of which are important, particular focus should be given to: (1) democracy and rule of the law, (2) human rights and fundamental freedoms,

⁸⁹ Ibid art 85.

(3) economic and social reform, (4) trade liberalisation of services, and (5) information and communication technologies.⁹⁰

In relation to the priority of democracy and rule of the law, the Action Plan requires Jordan to establish a political dialogue between the Jordanian Parliament and its EU counterpart. In addition, Jordan must improve good governance and transparency in accordance with international standards that have been recognised by Jordan (for example, UN Conventions). In the medium term, the Action Plan requires that Jordan promote national dialogue on democracy, reform legislation related to political parties and elections, and adopt plans and programs for public sector reform.⁹¹

On the priority of human rights and fundamental freedoms, Jordan is required by the Action Plan to support the freedom of the media and permit greater freedom of expression, to promote freedom of association and reform the legislation on association, to enhance the protection of children's rights and eliminate child labour, and to promote equal treatment of women. To implement these requirements, Jordan needs to introduce new legislation and/or incorporate into national law the provisions of a number of international treaties to which Jordan is party.⁹²

On the priority of economic and social reform, the Action Plan requires that Jordan take the necessary steps to reduce public debt, improve public finance

⁹⁰ European Commission, *EU/Jordan Action Plan* <http://ec.europa.eu/world/enp/pdf/action_plans/jordan_enp_ap_final_en.pdf> at 3 September 2009.

⁹¹ *Ibid* 2.1(1).

⁹² *Ibid* 2.1(5).

management and transparency, and increase efficiency of the public sector. The Action Plan also requires Jordan to support the privatisation program, to promote local and foreign investment in Jordan, and to adopt a national strategy to address poverty and unemployment issues.⁹³

In relation to prioritising trade liberalisation of services, the Action Plan requires that Jordan gradually abolish any restrictions on the supply of services by establishing the Euro-Med Framework Protocol,⁹⁴ developing a strategy to enhance competitiveness (for example by simplifying regulations and facilitating administration), supporting Jordan's preparation for future liberalisation of trade in services in selected sectors; and enhance services supply by developing necessary administrative structures and removing any barriers identified.⁹⁵ For example, in regard to the development of financial services, Jordan is required to review its current regulatory framework and created and train independent authorities to ensure effective supervision; and in regard to further development of capital markets, and liberalisation of current payments and capital movements,⁹⁶ Jordan must review current legislation to assess the need for further liberalisation of these areas and

⁹³ Ibid 2.2.

⁹⁴ For text, see the *Protocol to the Euro-Mediterranean Agreement Establishing an Association between the European Communities and their Member States, of the One Part, and the Kingdom of Morocco, Morocco, of the Other Part, to Take Account of the Accession of the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia, and the Slovak Republic to the European Union* [2005] OJ L 242/2

<<http://ec.europa.eu/world/agreements/downloadFile.do?fullText=yes&treatyTransId=2381>> at 4 February 2011.

⁹⁵ *EU/Jordan Action Plan*, above n 90, 2.3.2(25).

⁹⁶ Ibid 2.3.3(26).

'guarantee the free transaction movement of capitals relating in particular to direct investment and the protection of foreign investment'.⁹⁷

On the priority of information and communication technologies, the Action Plan requested that Jordan to: (1) elaborate a national policy on the development of the sector including regulatory, economic, technological and social aspects. (2) liberalise the market for fixed voice telephony, (3) develop a regulatory framework that includes (among other considerations) universal service, users rights, privacy protection and data security, and (4) implement government plans including e-Transaction law and projects such e-government, e-commerce and e-finance in Jordan.⁹⁸

The implementations of the above priorities included in the Action Plan are subject to annual assessment and monitoring by the EU. The 2008 Progress Report on Jordan by the EU reveals that Jordan has made mixed progress in this regard.⁹⁹ For example, on the issue of elections as part of democracy and the rule of law, Jordan still needs to draft a modern law for parliamentary elections and needs to establish an independent committee to monitor and supervise the elections, while on the issue of fighting against corruption, and with the technical assistance provided by the EU, Jordan has made progress by establishing the Anti-Corruption Commission (ACC) in January 2008.¹⁰⁰

⁹⁷ Ibid 2.3.3(27).

⁹⁸ Ibid 2.5(56).

⁹⁹ Commission of the European Communities, 'Implementation of the European Neighbourhood Policy in 2008: Progress Report Jordan' (2009) Report No SEC (2009) 517/2, <http://ec.europa.eu/world/enp/pdf/progress2009/sec09_517_en.pdf>.

¹⁰⁰ ACC established in accordance with *Anti-Corruption Commission Law No 62 of 2006* (Jordan) [Arabic] *Official Gazette*, No 4794, on 30 November 2006, at 4534.

The ACC has the authority to investigate complaints and refer them to court.¹⁰¹

On the issue of human rights and fundamental freedoms, the Progress Report on Jordan noticed limited progress in some areas and good progress in others. For example, the *Family Protection Law of 2008*¹⁰² was enacted to protect women from violence, and hospital, schools, and community centres have an obligation to report suspected cases of abuse to the authorities. However, the law fails to explicitly criminalise domestic violence, and fails to increase punishments for so-called 'honour crimes'.¹⁰³

On the issue of economic and social reform, the Progress Report reveals some progress has been made in Jordan concerning business opportunities, the right of establishment, and free movement of goods. However, the Report shows that Jordan still suffers from poverty with 14.5 per cent of the population living below the poverty line.¹⁰⁴

To sum up, a comparison of JUSFTA and Jordan-EU AA is revealing.

1. At the outset, it is important to admit that the US and the EU are great economic and political powers. Therefore, Jordan's relationship with these two giants is not equal, but rather both are needed by Jordan.
2. The JUSFTA deals with specific economic issues, while the AA extends its provisions to include political, economic, social and cultural issues.

¹⁰¹ Commission of the European Communities, 'Implementation of the European Neighbourhood Policy in 2008: Progress Report Jordan' (2009) Report No SEC (2009) 517/2, at 3.

¹⁰² *Family Protection Law No 6 of 2008* (Jordan) [Arabic] *Official Gazette*, No 4892, 16 March 2008, at 821.

¹⁰³ Commission of the European Communities, 'Implementation of the European Neighbourhood Policy in 2008: Progress Report Jordan' (2009) Report No SEC (2009) 517/2, at 5.

¹⁰⁴ *Ibid* 9.

The AA has greater influence on the lives of Jordanian as it may interfere with their core values (for example, issues related to family and women).

3. The AA aims to establish a free trade area with Jordan by 2014, subject to Jordan implementing the obligations included in the Action Plan. There is a possibility that the EU may refuse to enter into free trade negotiations with Jordan if the latter party fails to meet some of its obligations under the Action Plan.

With regard to privacy, Jordan has not yet made any progress in drafting legislation or regulations in the area of privacy protection and data security as requested by the Action Plan. The author suggests that Jordan's current position on privacy protection may be explained on the basis that Jordan is more committed to the JUSFTA than to the AA. Jordan may favour the US position on privacy which primarily seeks to protect commercial interests rather than promote privacy. As stated above, the US sees privacy protection laws as a barrier to flow of information, a barrier that would adversely affect international trade. This suggestion may be supported by examining Jordan's position to privacy protection in one of the most liberalised sectors in the country — the telecommunications sector. Jordan's approach to privacy protection in the telecommunications sector in Jordan has not been developed in accordance with the Association Agreement. The next section examines this sector and its privacy regulations, where applicable.

5.3 The Telecommunications Sector in Jordan

Globally, there is no sector that has undergone more rapid change in the past two decades, in terms of new technologies and policies, than the telecommunications sector.¹⁰⁵ This is the result of a number of phenomena, including the rapid evolution of technology, the introduction of many new services, the liberalisation of the market and the privatisation of many government owned networks (as discussed above).¹⁰⁶

At the national level, the Jordanian telecommunications sector has witnessed significant changes in many aspects including: the adoption of regulatory policies, a government commitment to liberalise the telecommunications market (Jordan was the first Arab country to fully liberalise this sector), the adoption of a deregulation process, and the readiness of the Jordanian market to introduce new and advanced services to meet the needs of businesses and consumers in this sector.¹⁰⁷ Further, with private sector help to build a dynamic, sophisticated communications infrastructure,¹⁰⁸ the telecommunications sector is set to become a key industry for the Jordanian economy with 10 per cent contribution to GDP in 2006.¹⁰⁹

Liberalisation of the telecommunications sector is one of the most noticeable changes that have occurred and has led to many positive impacts on Jordan's

¹⁰⁵ Kelley Lee, *Global Telecommunications Regulation: A Political Economy Perspective* (1996) 1.

¹⁰⁶ Natasha Finlen, *Consumer Protection in the Australian Telecommunications Market-Post July 1997* (Legal Research Project Thesis, Macquarie University, 1997) 3.

¹⁰⁷ Telecommunications Regulatory Commission (TRC), 'Annual Report 2007' (2007) 12 avail <www.trc.gov.jo>.

¹⁰⁸ MoICT, *Invest in ICT in Jordan* (2005) Ministry of Information and Communications Technology <<http://www.jordanecb.org/pdf/InvestinICTinJordan.pdf>> at 16 April 2009, 12.

¹⁰⁹ Ministry of Information and Communications Technology, *The e-Readiness Assessment of The Hashemite Kingdom of Jordan 2006* (2006) MoICT <http://www.moict.gov.jo/MoICT_Jordan_ereadiness.aspx> at 26 June 2009.

economy, particularly on the ICT sector. Prices of services in this sector have decreased, the number of internet services (ISPs) and communication product suppliers has increased, and foreign telecommunications products are now freely imported into Jordan. Further, consumer demand for telecommunications services in key services sectors such as financial and banking services have increased.¹¹⁰

Figure 2 below shows that in year 2009 there were 6.01million mobile phone customers in Jordan, which is equivalent to a penetration rate of 101 per cent, representing an increase of 44 per cent since year 2005. Business Monitor International predicted that over 8.45 million mobile users by the end of 2013, giving a penetration rate of almost 120 per cent.¹¹¹ The ongoing growing number of mobile users in Jordan as reflected in Figure 2 is a clear evidence of the impact of the liberalisation program on the telecommunications sector in Jordan. Liberalisation facilitated strong competition between local and foreign telecommunications companies which resulted in a significant drop in mobile prices, thus making them more accessible to a more people and resulting in an increased uptake of the technology.¹¹²

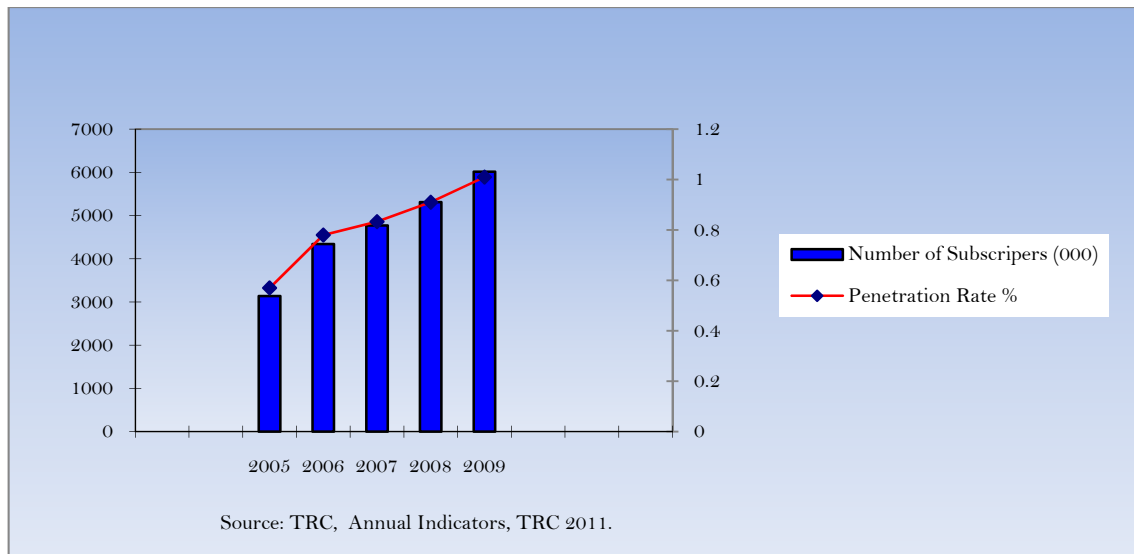
¹¹⁰ Ministry of Industry and Trade, 'Assessment of Trade in Services of the Hashemite Kingdom of Jordan, above n 25, pt II, 37.

¹¹¹ Business Monitor International, 'Jordan Telecommunications Report Q2 2009: Including 5-year Industry Forecasts' (2009) 21.

¹¹² Ministry of Information and Communications Technology, *The e-Readiness Assessment*, above n 109, 9.

Figure 2

Number of Mobile Subscribers and Penetration Rate (2005–2009)



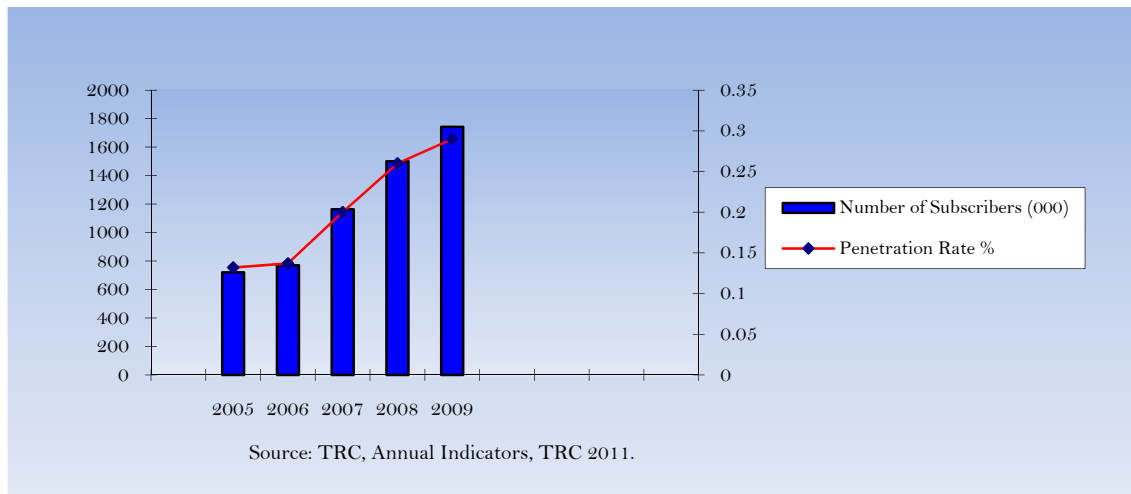
With respect to the internet users in Jordan, Figure 3 below shows a slight increase of the number of internet users. In 2009, the number of internet users was 1742 million with an increase of 15.8 per cent since year 2005. Although, this is still below desired levels due to on-going affordability issue, the number of internet users is expected to reach 3.066 million by the end of 2013. This would give a penetration rate for Internet usage of 43 per cent.¹¹³ A number of factors have been identified as obstacles to growing number of internet users including the high cost of internet access and of personal computers (PC) themselves and of related equipment (for example, software) and for repairs.¹¹⁴

¹¹³ Business Monitor International, 'Jordan Telecommunications Report Q2 2009, above n 111, 23.

¹¹⁴ Ministry of Information and Communications Technology, *The e-Readiness Assessment*, above n 109. .

Figure 3

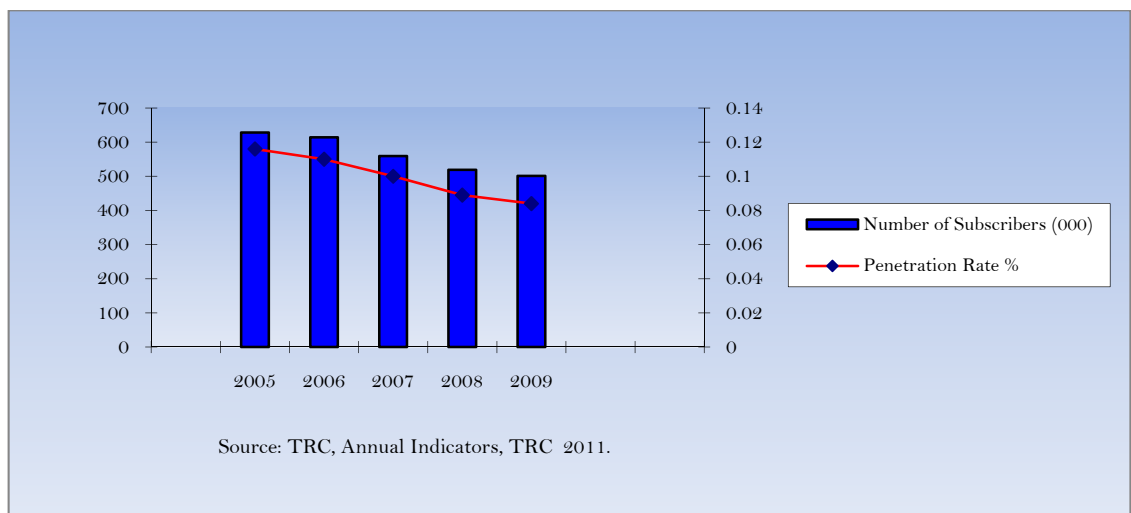
Number of Internet Subscribers and Penetration Rate (2005–2009)



Mobile for fixed substitution and the use of Voice Internet Protocol (VoIP) as well as the high cost of a fixed line have caused fixed line telephone services to drop. Figure 4 shows the number of fixed line subscribers has reached 614,000 customers which is equivalent to a penetration rate of 10 per cent.¹¹⁵

Figure 4

Number of Fixed line Subscribers and Penetration Rate (2005–2009)



¹¹⁵ Business Monitor International, 'Jordan Telecommunications Report Q2 2009, above n 111, 22.

The legal basis for Jordan's liberalisation of the telecommunications sector is the *Telecommunications Law No 13 of 1995*. By enacting this law; Jordan has made the first step in meeting its obligations under the GATS Agreement which requires the end of government ownership in telecommunications services. The law established two regulatory bodies to regulate and monitor the telecommunications services provided by licensed telecommunications companies. The next two sections provide a brief account of these governmental regulators and their roles.

5.3.1 The Ministry of Information and Communications Technology (MoICT)

Established in April 2002, the MoICT is the governmental entity responsible for articulating policy in the areas of IT, telecommunications, and post in Jordan. The Ministry's policy calls for market liberalisation, public-private partnership (PPP), and an end to government monopoly, which would include the government disposing of its majority shareholding in the telecom and postal sectors.¹¹⁶ The MoICT is charged with the developing, incubating, and supporting ICT initiatives at the national level, stimulating local and foreign technology investments, as well as promoting awareness of the significance of ICT and encouraging its use by all segments of the population.¹¹⁷ Furthermore, the MoICT is also responsible (in collaboration with other government agencies and to present them to the Council of Ministers) for the preparation of draft laws on telecommunications and

¹¹⁶ MoICT, *About the MoICT* (2003) Ministry of Information and Communications Technology <http://www.moict.gov.jo/MoICT_about_moict.aspx> at 25 June 2009.

¹¹⁷ Business Monitor International, 'Jordan Telecommunications Report Q2 2009, above n 111, 41.

information technology.¹¹⁸ Its role is to ensure that the ICT resources are exploited by Government entities in the most efficient way possible, consistent with best practices and free market principles.¹¹⁹ However, day-to-day regulation of Jordan's telecommunications and postal markets is delegated to the Telecommunications Regulatory Commission (TRC). The role of TRC in regulating the telecommunications market is now examined in detail.

5.3.2 Telecommunications Regulatory Commission (TRC)

Established in 1995 under the *Telecommunications Law No 13 of 1995*, the TRC is an independent agency. It is not responsible to the MoICT, but rather reports to the Prime Minister. The TRC's primary responsibilities are included within Article 6 of the *Telecommunications Law No 13 of 1995*.¹²⁰

Among those responsibilities are:

- a) To regulate telecommunications and information technology services in the kingdom in accordance with the established general policy so as to ensure the provision of high quality telecommunications and information technology services to beneficiaries at reasonable prices; and, by doing so, to make possible the optimal performance of the telecommunications and information technology sectors.

.....

- d) To protect the interests of Beneficiaries and monitor the actions of persons and licensed parties to ensure that the conditions of Licenses are observed, including specified services standards, service quality, and prices and to take necessary actions in this regard and to penalise those who violate these conditions.

.....

- e) To stimulate competition in the telecommunications and information technology sectors, relying on market forces and so regulating them as to ensure the effective provision of telecommunications and information technology services and to ensure

¹¹⁸ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002* (Jordan) art 3(k).

¹¹⁹ Ministry of Industry and Trade, 'Assessment of Trade in Services of the Hashemite Kingdom of Jordan, above n 25, 27.

¹²⁰ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002* (Jordan).

that its regulation is sufficient and effective to forbid or curtail illegal competitive practices prevent any person with a dominant position in the market from abusing his position, and to take all necessary actions in this regard.

.....

g) To encourage self-regulation by the telecommunications and information technology sectors.

.....

p) To propose draft laws dealing with the telecommunications and information technology sectors, escalate them to the MoICT, and prepare the by-laws and established the instructions related thereto.¹²¹

The above responsibilities grant the TRC an exclusive authority over a set of issues such as: licensing of ICT services, consumer protection, protection of interests for individuals, market competition and most importantly, the authority to regulate laws and issuing instructions to address arising issues in the telecommunications sector.

With respect to the issue of licensing, Article 12(a) of the *Telecommunications Law of 1995* authorises the TRC to grant licences for the following:¹²²

- To build, operate, and manage Public Telecommunications Networks and to provide Telecommunications Services to Beneficiaries,
- To build, operate, and manage Public Telecommunications Network, or
- To provide Telecommunications Services to Beneficiaries.

As of the end of 2009, Jordan had a total of 78 telecommunications service providers. An individual licence issued for 24 public telecommunications service providers who require the use of scarce resources (radio frequency spectrum, public rights of way, and telephone numbers). A class licence

¹²¹ Ibid.

¹²² Ibid.

issued for 54 public telecommunications service providers who do not use those scarce resources.¹²³

With regards to market competition, the TRC has been influential in allowing multinational (local and foreign) telecommunications service providers to operate in Jordan and provide a variety of services and products such as: mobile telephone services, land line telephone services, internet, paging services, data networks, prepaid telephone cards and public pay phones. Currently, there are three major telecommunication companies providing such services and products: Zain (with its parent company based in Kuwait), MobileCom (a subsidiary of Jordan Telecom), and Umniah (a subsidiary of Batelco Bahrain). In addition, there is the New Generation Telecommunications Company, Xpress, a company licensed to provide radio trunking services, SMS and other information services.

The role of the TRC is to draft laws and issue instructions to address any arising matters. This is an important role. For example, in response to public pressure, the TRC has issued a set of instructions to prevent the sending of bulk SMS (Short Message Service) to individuals (mobile phone users). These instructions provide individual with the following protections:¹²⁴

¹²³ Telecommunications Regulatory Commission (TRC), 'Annual Report 2009' (Telecommunications Regulatory Commission (TRC), 2009) 65, Appendix (3). Text avail: <www.trc.gov.jo>.

¹²⁴ Instruction to Regulate Sending of Bulk SMS, Board of Commissioners (TRC), Decision No 3, 4 January 2011 (Jordan) [Arabic], issued in accordance with Article 6(a) (d) and Article 58 of the *Telecommunications Law No 13 of 1995* (Jordan) <http://trc.gov.jo/images/stories/pdf/Instructions_to_Regulate_Bulk_SMS_09012011.pdf?lang=english> at 15 December 2010.

1. Telecommunications service providers must provide individuals, free of charge, with an easy and accessible mechanism to request a stoppage on receiving SMS.
2. Telecommunications service providers must not send SMS to individuals who wish to opt out.
3. Telecommunications service providers must not send SMS to individuals who opted out which has been originated from a third party.
4. Telecommunications service providers must not send SMS to individuals on a public holiday and on weekdays between 9am–7pm.

Although these instructions are a step in the right direction in the area of privacy protection in the telecommunications sector in Jordan, the author believes that they suffer from a number of shortcomings that make them insufficient to protect individual privacy in this sector. These shortcomings are:

- (1) They are only applicable to one type of telecommunications services, namely telemarketing via SMS, and do not extend their application to telemarketing via telephone calls or e-mails.
- (2) The current instructions give individuals the right to opt out rather than opt in. As discussed earlier in Chapter Four, an effective opt-out method relies upon individuals being able to understand how telecommunications service providers are using their personal information. It also relies upon individuals being informed that they have the right to opt-out of this information practice (that is, receiving SMS).

(3) The application of these instructions does not extend to government agencies, which means that governmental departments and their affiliates (private entities) can still send unwanted SMS to individuals.

The author believes that the above instructions adopted by the TRC are insufficient to protect individual privacy in the whole telecommunications sector in Jordan. In order to propose an alternative comprehensive and adequate regulatory framework for privacy protection, a number of telecommunications service providers in Jordan are subjected to investigation to identify individual privacy concerns within this sector in relation to its adoption and use of ICTs.

5.3.3 The Privacy Implications in the Telecommunications Sector in Jordan

As stated above, the TRC in Jordan has issued licences to 78 telecommunications service providers as at 31 December 2009.¹²⁵ These companies handle personal information about their customers in order to supply them with services and products, including landline telephone services, mobile telephone services, internet services, and pre-paid telephone cards.¹²⁶ A number of these companies were chosen for a case study for an investigation regarding the issue of privacy. The study adopts the following method.

¹²⁵ Telecommunications Regulatory Commission (TRC), 'Annual Report 2009, above n 123, 65.

¹²⁶ Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008) V3, 2377.

5.3.3.1 An Online Case Study

An online method was utilised in a survey conducted during 10 to 25 September 2009 to examine privacy policies/statements on a sample of 9 telecommunications service providers listed in Table 5 below.¹²⁷ The remaining companies with an online presence in Jordan were excluded from this study because their websites either could not be accessed via online (for example, due to technical difficulties) or because these companies do not have privacy policies/statements on their websites. The purpose of this study is to measure whether or not these privacy policies/statements implemented by telecommunications companies in Jordan provide adequate protection to individual privacy. The privacy policies/statements are the only available provisions concerning individual personal information that can be assessed in this context. Jordan's lack of privacy legislation or regulation to deal with the privacy issue, and particularly, in the telecommunications sector is the driving force behind this study.

The adequacy of these privacy policies/statements is measured against the principles of the Information Practice Privacy Principles (FIPs). These principles are: (1) Notice, (2) Choice, (3) Access, (4) Security, and (5) Enforcement. The reason for using the FIPs as the benchmark for this study is because they were developed to become a cornerstone of the self-regulation regime. As claimed above, the telecommunications sector in Jordan chose the self-regulation approach to protect personal information. This is documented in the Jordan-US Joint Statement on e-Commerce and in

¹²⁷ See Appendix B, Exhibits 1–9.

the Statement of Government Policy 2007 on the ICT & Postal Sectors. One way to implement such approach is for telecommunications companies to introduce privacy guidelines on the form of policies/statements.

Table 5
Telecommunications Companies in Jordan with FIP Principles

Company Name	Ability of Collecting, Using & Transferring of Personal Information	Availability of FIP Dimensions				
		Notice	Choice	Access	Security	Enforcement
1. Jordan Mobile Telephone Services Company http://jo.zain.com/English/Pages/ZainPrivacyPolicy.aspx	Yes	Yes	Yes	Yes	Yes	No
2. New Generation Telecommunication Company http://www.xpress.jo/terms/terms-policies.asp	Yes	Yes	No	No	No	No
3. Umniah Mobile Company http://www.umniah.com/umniah/Templates/terms/PrivacyPolicyAr.shtm	Yes	Yes	Yes	Yes	Yes	No
4. Orange Telecom http://www.orange.jo/en/index.php	Yes	Yes	Yes	Yes	Yes	No
5. Tarasol Telecom http://www.tarasol.jo/privacy-policy	Yes	No	No	No	No	No
6. Al-Moakhaha Lilkhadamat Al-Logisteiah http://www.xol.jo/PrivacyPolicy.aspx	Yes	Yes	Yes	Yes	Yes	No
7. Middle East Communication Corporation http://www.mec.com.jo	Yes	Yes	No	No	No	No
8. Sama Telecom www.sama.jo	Yes	No	No	No	No	No
9. Al-Raeh Li Khadamat Al-Lttisalat http://www.aa-telecom.com/dev/privacy.php	Yes	Yes	Yes	Yes	Yes	No
Percentage of Telecommunications Company with FIP Principles	100%	77.7%	55.55%	55.55%	55.55%	0.00%

The online study examines the following issues:

1. Do telecommunications companies in Jordan collect use, store, and transfer customers' personal information?
2. Do telecommunications companies in Jordan have one standard privacy policy/statement?
3. Do these privacy policies/statements meet the standards of the FIPs? and,
4. How do telecommunications companies in Jordan attend to customer complaints in regard to their privacy?

Table 5 above reveals that all 9 or 100 per cent of the telecommunications companies whose online presence has been here surveyed have the ability through their websites to collect customers' (visitors) personal information. This practice can occur when customers use hyperlinks such as 'Contact us', 'Sign Up', 'Register', or 'Suggestions & Complaints'. The use of these hyperlinks enables companies to collect personal information including: name, postal address and contact details (telephone number and email addresses).

The survey also shows that some companies placed information regarding their information privacy practices under the name of 'privacy policy' while other companies preferred the term 'privacy statement'. The difference between privacy 'policy' and privacy 'statement' is that a privacy statement communicates company's information practices to the public while privacy 'policy' describes company's standards for the collection of personal information and this information is used and managed by the company.¹²⁸ This difference may lead to

¹²⁸ William G Staples (ed), *Encyclopedia of Privacy* (2007) vol II, 427.

the conclusion that these privacy policies/statements may have been obtained from different sources.

Table 5 also shows that privacy policies/statements placed on the home page of the telecommunications companies surveyed do not have standard provisions to address the issues included in the FIPs. These issues are:

a) Notice

The online study shows that 7 of the 9 websites surveyed (or 77.7 per cent) have information related to the 'notice' dimension. As stated in the previous chapter, this dimension is considered by the US FTC as the most fundamental dimension of the privacy policy/statement. Without a notice, an individual cannot make an informed decision as to whether or not and to what extent personal information is to be disclosed.¹²⁹

b) Choice

With regard to the dimension of choice, the above study shows that only 5 of the 9 companies assessed (or 55.55 per cent) provide individuals with choices regarding the use of their personal information. The availability of this offers individuals the option to whether or not their information can be used or collected personal information disclosed to third parties.

c) Access

With regard to the principle of access, the study also shows that the same number of companies, that is 5 of the 9 surveyed (or 55.55 per cent) give individuals a right to access to their information. These companies provide individual with information on how to correct or amend their personal information.

¹²⁹ Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) Federal Trade Commission <<http://www.ftc.gov/reports/privacy3/priv-23a.pdf>> at 4 March 2010.

d) Security

With regard to the principle of security, 5 of the 9 telecommunications companies listed in Table 5 above (or 55.55 per cent) have made reference to the issue of data security. Such a reference informs individuals as to how the security of personal information is maintained by the company concerned. It also urges individuals to take all necessary actions to ensure the safety of their personal information when such information is transmitted through company websites (with such actions including, for example, regularly changing their password, the use of a secure browser).

e) Enforcement

One of the most surprising findings is that none of the 9 companies examined included in their privacy policies any information (for example, contact details) to individuals regarding access to an independent agency that could enforce their privacy rights. Only general information was available, namely that for individuals who wished to contact the company if they had any complaints concerning their personal information. Individuals must have access to an independent enforcement mechanism that is free of charge, fast and effective – and preferably via the website of the communications companies themselves rather than rely on consumer knowledge of their rights and of independent avenues of complaint.

In summary, a number of comments can be made from the above study:

1. All of the telecommunications companies in Jordan surveyed above do not have similar provisions in their privacy policies/statement. This may create a discrepancy and confusion for individual service users. Therefore, privacy policies/statements should clearly outline a company's information practices.

The privacy policy/statement should be written in clear and easy to understand language by a non-specialist person.

2. All telecommunications companies represented in the above table collect personal information, however, they should collect only the information that is a necessity to proceed or complete a transaction. Any collection of non-essential information should be optional.
3. Privacy policies/statements should clearly state that personal information submitted by children and young individuals is not required to access to their websites. Any information obtained by telecommunications companies about children should be deleted immediately.
4. A company should obtain prior consent before transferring personal information to another company as a result of dissolving, merging with a new company, or changing its legal status.
5. In addition to having an enforcement mechanism, a telecommunications company should make available specific information relating to the management of personal information. It is recommended that a telecommunications company establish a specific position, namely a privacy officer, who is responsible for the company's compliance with its privacy policy/statement.

5.4 The Banking Sector in Jordan

5.4.1 Introduction

The reform of the financial sector in Jordan began in the late 1980s as part of the liberalisation process. The authors of an IMF working paper place Jordan amongst the nations receiving the highest financial development scores in the Middle East-

North Africa (MENA)¹³⁰ region, largely due to the liberalisation processes it has undertaken.¹³¹

The reform to the financial sector was significant in terms of social and economic impacts of the ICT advancements in Jordan. Currently, the majority of banks, if not all, have carried out radical improvements to their services in conformity with these advancements. The banks in Jordan are very competitive in providing their customers with services using the latest technologies including: internet banking, phone banking, SMS, ATM services and mobile phone banking. These technologies offer convenience to customers in terms of ease of customer access to their accounts, transactions, and communications about their accounts. It also reduces bank costs. The reduction of the need for cash on hand and paper when using the computerised banking system also reduces the need for property and employees.¹³² For example, the application of successive generations of computerisation since the early 1960s has dramatically reduced 'back-office' staff levels, while the growth of expensive paper-based systems for money transmission has been curtailed by the development of effective paperless computerised payment systems.¹³³

However, e-banking services imply a number of privacy implications. It enables banks to store a large amount of personal financial information on databases and

¹³⁰ The MENA region covers the Islamic State of Afghanistan, Algeria, Bahrain, Djibouti, Egypt, the Islamic Republic of Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, the Syrian Arab Republic, Tunisia, the United Arab Emirates, West Bank and Gaza, and the Republic of Yemen.

¹³¹ Susan Creane et al, 'Financial Sector Development in the Middle East and North Africa' (International Monetary Fund, 2004) 13, 18 <<http://www.imf.org/external/pubs/ft/wp/2004/wp04201.pdf>>.

¹³² Alan Tyree and Prudence Weaver, *Weerasooria's Banking Law and the Financial System in Australia* (6th ed, 2006) 82.

¹³³ Brian Anderton et al, 'The Impacts of Information Technology on the Financial Services Sector' in Brian Anderton (ed), *Current Issues in Financial Services* (1995) 68. See also Creane et al, above n 131, 38.

computers. This information can be easily shared with third parties. For example, they information about individuals' habits or preferences (revealed by purchases on credit cards) would be able to be shared. The use of e-banking services may increase the risk of identity fraud, as the information necessary to establish an identity is aggregated at a single location, which, if criminals access that site, identity theft becomes easier. Further, government agencies are able to access and monitor individual's financial personal information in the name of fighting money laundering and terrorism activities or illegal drugs. There is a possibility that government activities in this regard may threaten the right to privacy of individuals.

The following sections attempt to identify the privacy implications or concerns raised by the rapid adoption of ICT in the banking sector of Jordan. The most recent developments that have occurred in the Jordanian banking sector are first examined. The types of services offered to bank customers in Jordan through the online environment are also listed. Then, the results of an online study conducted in order to examine the privacy policies/statements of the e-banking adopted the banks operating in Jordan are revealed. The online study gives particular attention to the privacy practices of the foreign banks in Jordan. The final section then provides analytical summaries regarding individual privacy protection in the context of e-banking.

5.4.2 The Banking System in Jordan

Banking in Jordan can be traced back to the early 1900s with the establishment of the 'Ottoman Bank' in 1925. Soon afterwards the largest commercial bank

Palestinian bank, 'The Arab Bank', was relocated to Amman as a result of the 1948 Arab-Israeli War.¹³⁴

The number of banks operating in Jordan at the end of 2009 stood at 23, of which two are Islamic banks and eight are branches of foreign banks. These banks carry out their operations through a domestic network of 593 branches and 67 representative offices. The ratio of population to total number of branches of operating banks currently stands at about 9.9 thousand citizens per branch. On the other hand, branches of the Jordanian banks operating abroad number 135 with an additional 26 representative offices.¹³⁵

The *Banking Law* gives the Central Bank of Jordan (CBJ) the authority to license banks wishing to operate in Jordan. The CBJ as the supervisory and regulatory authority of the banking system enjoys the status of an independent institution with considerable authority delegated to it.¹³⁶ In 2006, for example, the CBJ issued a regulation to combat money laundering and the financing of terrorism and to maintain the integrity of the Jordanian banking system.¹³⁷

Licensed banks may engage in the following financial activities, without being required to specialise: accepting deposits, granting credit, including financing commercial transactions; providing payment and collection services; issuing and administering instruments of payments (for example, bank acceptance; debit and

¹³⁴ Capital Investments, *Banking Sector Report* (2009) Capital Investments <<http://www.capitalinv.jo/files/Banking%20sector%20Report-%204%20January%202009.pdf>> at 1 October 2009.

¹³⁵ Central Bank of Jordan, *Annual Report 2008* (2008) Central Bank of Jordan <<http://www.cbj.gov.jo/uploads/chapter2.pdf>> at 30 September 2009.

¹³⁶ *The Central Bank of Jordan Law No 23 of 1971* (Jordan), *Official Gazette*, No 2301 25 May 1971 arts 3, 4.

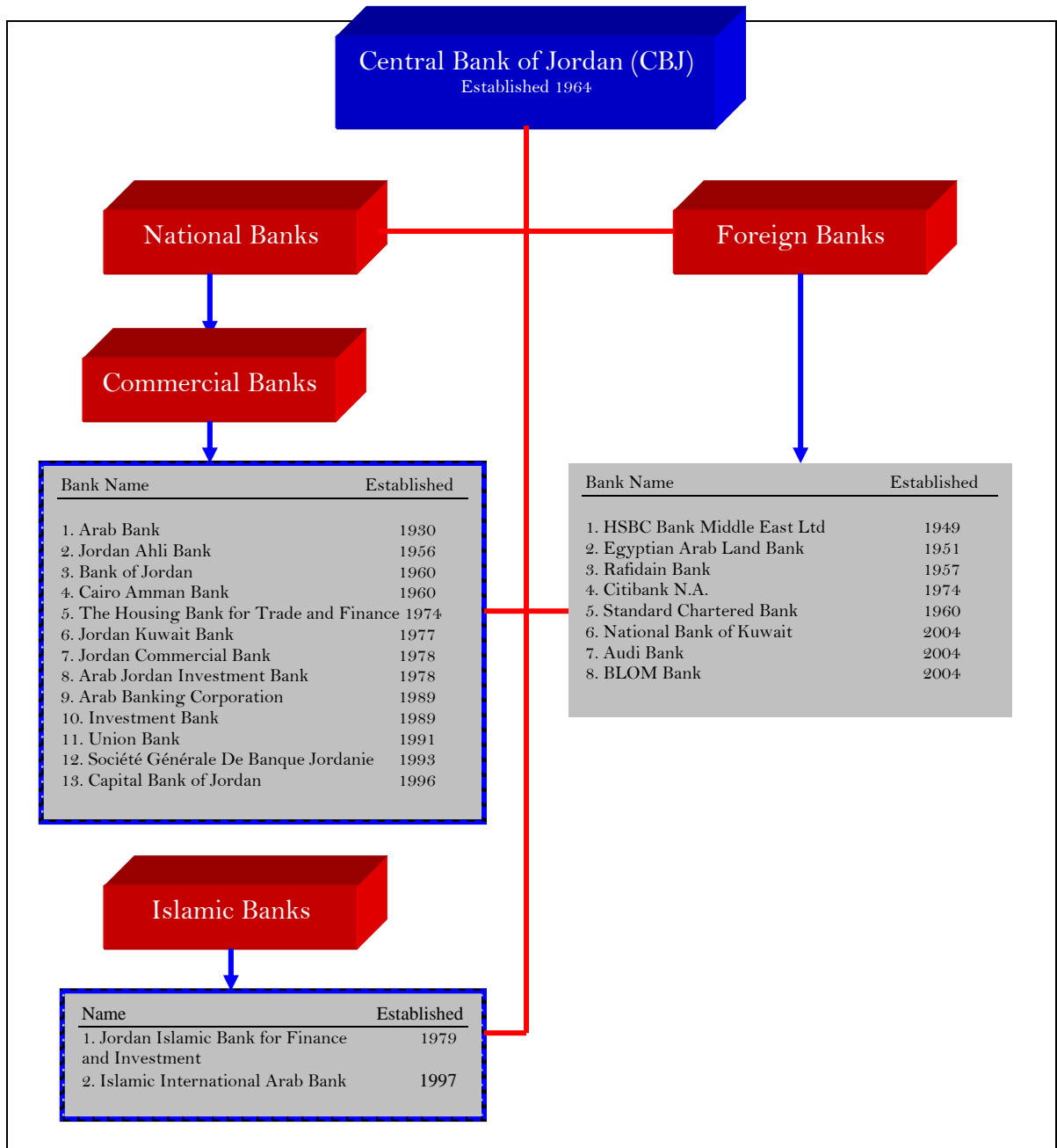
¹³⁷ *Regulations of Anti-Money Laundering and Terrorism Financing Circular No 29 of 2006* (Jordan). <<http://www.cbj.gov.jo/uploads/AML.pdf>> at 20 July 2010. (Issued pursuant to Article 99(b) of the *Banking Law*).

credit cards, and travellers' cheques; and dealing in selling and purchasing of money and capital market instruments on its own account or on behalf of customers' accounts, and so on). Banks in Jordan can also manage fund investments; provide financial advisory services, safekeeping of securities and valuable items, and any other related banking activities approved by the Central Bank.¹³⁸ The establishment of subsidiaries by banks engaging in non-banking financial services is subject to approval by the Central Bank. For instance, Bank Audi of Lebanon was the first bank to obtain a licence for combined banking and insurance services. Figure 5, below, provides an overview of the banking system in Jordan as of 2009. It consists of the Central Bank of Jordan, 13 local banks which 2 banks are established in accordance with *Shari'ah* (Islamic law) and 8 foreign banks owned by international investors.

¹³⁸ *Banking Law No 28 of 2000* (Jordan) art 37.

Figure 5

Jordan Banking System - as at 30 December 2009



Source: CBJ, Annual Report 2009, the Banking System

5.4.3 The Banking System and ICT in Jordan

Worldwide, various information and communication technology channels have emerged to enhance the speed and quality of service delivery and radically change

how banking services are being conducted.¹³⁹ The use of electronic delivery channels for banking products and services has defined the concept of 'electronic banking'.¹⁴⁰ There are a number of electronic delivery channels; however, the focus of this section will be on the following: (1) Automatic Teller Machines (ATMs) (2) Internet Banking, (3) Phone Banking, and (4) Credit Cards. These four channels are largely available for use by the customers in Jordan.

5.4.3.1 Automated Teller Machines (ATMs)

Automated teller machines (ATMs) are used to perform and facilitate a number of transactions including, but not limited to, cash withdrawals and cash deposits, the transfer of funds between accounts of the cardholder, to address account balance inquiries, to make bill payments or in the approval process for simple loans. Most of the ATMs are sited in exterior walls of financial institutions enabling customer access to their accounts without the need to actually enter the building. Although transaction details are transmitted electronically to a financial institution's computer for the adjustment of accounts, the main purpose of an ATM transaction is usually not the electronic transfer of funds between accounts, but the supply of currency (notes) to a customer. The ATM terminal validates the user's identity, provides the currency requested, and transmits details of the transaction to the bank to enable the account to be debited.¹⁴¹

¹³⁹ Akinlolu Agboola and Oyesola Salawu, 'Optimizing the Use of Information and Communication Technology (ICT) in Nigerian Banks' (2008) 13(1) *Journal of Internet Banking and Commerce* 1, 3.

¹⁴⁰ Andrea Schaechter, 'Issues in Electronic Banking: An Overview' (International Monetary Fund, 2002) 3.

¹⁴¹ Olujokè Akindemowo, *Information Technology Law in Australia* (1999) 99–100.

ATMs were first used in Jordan in the early 1980s. At the end of 2010,¹⁴² there were 1023 ATMs in many different places all over the country, with sites now including shopping centres, hospitals, universities and of course, bank branches.¹⁴³ ATM services are services that every bank in Jordan must provide for their customers. However, the specifications of the ATM cards vary from one bank to another. For example, the Jordan Kuwait Bank has distributed to their customers new ATM cards called 'Visa Electron' to replace traditional ATM cards. The card is valid for cash withdrawal from any ATM in Jordan and abroad bearing the Visa logo. It is also good for use at points of sale (POS) to purchase items from any store around the world.¹⁴⁴

5.4.3.2 Internet Banking

This form of e-banking allows customers to conduct different types of transactions using the World Wide Web browser (www). Customers can view their balances, transfer funds between accounts, pay bills, and make purchases from any location around the world.

Internet banking is banking through 'open' communication channels. The messages sent between customers and banks are not only subject to interception, but subject to interception by an unknown and unknowable class of 'listeners'. The path by which the message is sent is not known in advance. The message may pass through and/or be stored in any number of computers.¹⁴⁵ Internet banking,

¹⁴² Suliman Abu-Khasabeh, 'ATMs in Jordan', *Manabar Alrai* (Amman), 24 December 2010, [Newspaper Article] [Arabic], <<http://www.manbaralrai.com/?q=node/92420>> at 19 January 2011.

¹⁴³ Association of Banks in Jordan, 'Development of the Jordanian Banking Sector' (Association of Banks in Jordan, 2008) 17, avail www.abj.org.jo at 2 April 2009.

¹⁴⁴ Jordan Kuwait Bank, *Visa Electron to Replace Traditional ATM Cards* (2000) Jordan Kuwait Bank <<http://www.jordan-kuwait-bank.com>> at 07 October 2009.

¹⁴⁵ Alan L Tyree, *Digital Cash* (1997) 10.

however, has advantages over traditional banking. An Internet financial institution reaches thousands of customers without needing expensive local branches. Online transactions cost less than one-tenth of ‘over-the-counter’ transactions.¹⁴⁶

For example, the Arab Bank was the first bank in Jordan to launch internet banking services in May 2000. In addition, the bank provides its customers — upon request — with an Internet Shopping Card (ISC). It is a plastic card that contains the cardholder’s name, card number, Card Validation Value (CVV), and the expiry date. This card can be used for shopping via online, telephone or mail orders. The customer can apply for this card over the internet, where the cardholder can also view balances and details of transactions. Although still essentially a credit card, the ISC is issued with a ‘smaller and separate limit from the primary Arab Bank Visa Credit Card’ for increased customer protection and security as the holder’s primary credit card may have a very generous limit and access to substantial cash advances.¹⁴⁷ The ISC limits the possible damage to the customer to the set maximum credit limit for the card.

Similarly, the Jordanian National (Ahli) Bank provides their customer with an ‘E-Com card’, which is a prepaid electronic card enabling its holder to purchase products via internet until the funds ‘preloaded’ onto the card are exhausted. The E-Com card has a limited amount of money ‘deposited’ to it but is able to be recharged within two years. Unlike the use of credit card, where limits may be high or transactions continued to be made after a limit has been reached, the use of the E-Com card can minimise the risks posed by fraudulent use by persons other

¹⁴⁶ Alan Tyree and Andrea Beatty, *The Law of Payments Systems* (Butterworths, 2000) 3.

¹⁴⁷ Arab Bank, *Internet Shopping* (2009) Arab Bank <<http://www.arabbank.com.jo/en/perscardinternet.aspx>> at 7 October 2009.

than the holder or identity theft due to the limited sum available to the cardholder.¹⁴⁸

Credit cards (see further below), debit cards, and preloaded cards remain vulnerable both to theft of the actual cards and to ‘skimming’ of the details on the cards at points of sale or at ATMs with such details able to be then transferred onto a ‘blank’ as well as to card details being obtained via ‘spyware’ (‘Trojans’) on the customer’s computer.¹⁴⁹

5.4.3.3 Telephone Banking

This form of e-banking enables customers to make enquiries and perform transactions by accessing their accounts over the telephone. The advancement of telecommunications in Jordan has enabled customers to use their mobiles to receive information on their banking transactions. Some banks in Jordan are currently providing their customers with information about their accounts via the Short Message System (SMS). For example, the Cairo Amman Bank implemented SMS in order to process customer requests, such as balance inquiry, last three transactions, and account statement request. The bank can also use the SMS to send information to customers such as account based notifications, account overdraft notifications and transaction based notifications.¹⁵⁰ In some instances, a number of banks are using the Wireless Application Protocol (WAP) to communicate with their customers.

¹⁴⁸ Jordan Ahli Bank, *The E-Com Card* (2009) Jordan Ahli Bank <http://www.ahli.com/prepaid_cards.shtm> at 7 October 2009.

¹⁴⁹ Australian Competition and Consumer Commission, SCAMwatch <<http://www.scamwatch.gov.au/content/index.phtml/tag/CardSkimming>> at 9 February 2011.

¹⁵⁰ Cairo Amman Bank, *SMS Banking* (2009) Cairo Amman Bank <www.cab.com.jo> at 7 October 2009.

5.4.3.4 Credit Cards

Credit cards are mainly issued by banks and allow for pre-arranged revolving credit up to an authorised limit.¹⁵¹ Banks operating in Jordan provide four types of credit cards, namely Visa, Master Card, American Express, and National Card. The number of credit cards granted by banks increased from 127,000¹⁵² in 2007 to 265,000 cards in 2008.¹⁵³ All banks in Jordan offer at least one type of credit card to their customers. For example, the Jordan Kuwait Bank offers their customers three types of credit cards Visa, Master Card and American Express and customers can apply for these cards by filling out an online application that is available on the bank's website.¹⁵⁴

5.4.4 The Privacy Implications of e-Banking in Jordan

E-banking services such as ATMs, credit cards (in addition to debit and EFTPOS cards), telephone banking, and on-line (internet) banking), provide alternative or additional methods for customers in Jordan to conduct various transactions (buy and sell goods, pay bills, obtain cash); however, a number of concerns related to privacy have arisen in relation to the use of these technologies. These concerns can be summarised as follow:

1. The above e-services have made it easier for banks to collect, store, and access large amounts of personal financial information. It has become easier to manipulate and aggregate this information as it machine-readable and machine-processable. As some of the e-services rely on the internet, it has become easier to physically locate individuals. For example, it is possible in

¹⁵¹ Tyree and Beatty, above n 146, 33.

¹⁵² Association of Banks in Jordan, '29th Annual Report 2007' (Association of Banks in Jordan, 2007) 15.

¹⁵³ Association of Banks in Jordan, 'The Annual Report of 2008' (Association of Banks in Jordan, 2008) 26.

¹⁵⁴ Jordan Kuwait Bank, *Individual: Credit Cards* <http://www.jordan-kuwait-bank.com/en/products_individual_cards.html> at 09 October 2009.

principle to locate an individual's use of an ATM, or to know details of his/her transaction as soon as it is completed. Similar observations can be made in regard to the use of credit or other POS transaction cards, the use of which can establish the purchasing patterns of banking customers in terms of goods and services. In addition to the a bank tracking patterns of transactions to better target marketing strategies for the bank, on-selling of such information to retailers by banks or by retailers or by third parties monitoring transactions (for example, via hacking/use of spyware) could pose a further threat to privacy.

2. Government surveillance of individual transactions is possible through the customer's use of e-services. The government may use e-services, as e-services becomes easier and cheaper to monitor transactions by individuals. This can be occurring if there are weak safeguards against government use of power. The government of Jordan is best known for issuing laws and regulation in the absence of a national parliament. In year 2009, there were 62 provisional laws issued by the government without rest of Parliament. This can be seen as an abuse of power by the Jordanian government.
3. Given the use of information supplied and derived from accounts, individuals should have the right to view, access, amend and correct their personal financial information generated by the methods used in e-services. For example, stored incorrect information may be used to deny individuals financial services such as the grant of a loan application or access to credit.

5.4.5 The Extent of e-Banking Services in Jordan

In order to identify and examine privacy concerns posed by the e-services in Jordan, the author conducted an online study of all banks operating in Jordan during the period from 1 September 2009 to 1 December 2009. A list of banks operating in Jordan was compiled, and their websites viewed to obtain information regarding whether they offered online services through the World Wide Web (www), and if so, what was the nature of these services. Table 6 (below) presents this information. It includes summary of the banks on-line services and, with respect to the privacy implications in the context of e-services, the privacy information practices of the listed banks are also summarised in the Table.

Table 6
Banks in Jordan and availability of Online Services and Privacy Policies/Statements

Bank Name	Website	Availability of Online Services	E-Banking	Sample of E-Services	Privacy Policy/ Statement
1. Arab Bank	www.arabbank.com.jo	Yes	Yes	E-Transfer Funds, SMS	Yes
2. Jordan Ahli Bank	www.ahli.com	Yes	Yes	Phone Banking, E-Com and Internet Banking	Yes
3. Cairo Amman Bank	www.cab.jo	Yes	Yes	Phone Banking, Internet Banking	Yes
4. Bank of Jordan	www.bankofjordan.com	Yes	Yes	Personal Loan, Car Loan and Credit Card	Yes
5. The Housing Bank for Trade & Finance	www.hbtf.com	Yes	Yes	Internet (Iskan) Online, (Iskan) SMS	No
6. Jordan Kuwait Bank	www.jordan-kuwaitbank.com	Yes	Yes	Loan Applications, Pre-Paid Mobile Cards	No
7. Arab Jordan Investment Bank	www.ajib.com	Yes	Yes	Credit Card Online Application-Visa	No
8. Jordan Commercial Bank	www.jgbank.com.jo	Inactive	Inactive	Unavailable	Unavailable
9. Jordan Islamic Bank	www.jordanislamicbank.com	Yes	Yes	Visa Smart Card, SMS	No
10. Jordan Investment & Finance Bank	www.jifbank.com	Yes	Yes	Internet Banking, ATM, Phone Banking	No
11. Arab Banking Corporation	www.arabbanking.com	Yes	Yes	ATM, Phone & Internet Banking and SMS	No
12. Union Bank	www.unionbankjo.com	Yes	Yes	E-Funds Transfer, ATM and SMS	No
13. Societe General Bank-Jordan	www.sgbj.com.jo	Yes	Yes	SMS, Internet Banking	No
14. Capital Bank	www.capitalbank.jo	Yes	Yes	Housing Loan, Personal Loan and Car Loan	No
15. International Islamic Arab Bank	www.iiab.com.jo	Yes	Yes	Internet Shopping Card, Phone Banking	No
16. HSBC Bank	www.jordan.hsbc.com	Yes	Yes	Credit Cards Online Application,	Yes
17. Egyptian Arab Land Bank	www.arakari.com.jo	No	No	Provide general information about the bank	No
18. Rafidain Bank	www.rafidian-bank.org	No	No	Provide general information about the bank	No
19. Citi Bank	www.citibank.com/jordan	Inactive	Inactive	Unavailable	Unavailable
20. Standard Chartered	www.standardchartered.com	Yes	Yes	E-Statement, E-Kiosk and Online Banking	Yes
21. Bank Audi	www.banqueaudi.com/jordan	Yes	Yes	Internet Banking	No
22. National Bank of Kuwait	www.nbk.com	No	No	Provide general information about the bank	Yes
23. BLOM Bank	www.blom.com/english	Yes	Yes	Internet Banking, ATM, SMS	No

Local Banks with Privacy Policy/Statement	4	30%
Foreign Banks with Privacy Policy/ Statement	3	37.5%
Islamic Banks with Privacy Policy/statement	0	0.00%

5.4.6 The Privacy Concerns for e-Banking in Jordan

In the context of e-banking, the Central Bank of Jordan is authorised by the Government to issue instructions to regulate the e-banking activities.¹⁵⁵ Whilst theoretically uniformity of direction could result; in effect this can result in further delegation and the possibility of inconsistency between banks in their practices. For example, the Payment System Regulations issued by the CBJ grant each bank in Jordan the authority to lay down its own policies to regulate the relationship between the bank and its customers in the context of e-banking.¹⁵⁶ Given this, the following section examines privacy concerns in the e-banking context and details how banks address these concerns.

Despite various benefits achieved by e-banking, such as low costs, greater efficiency and convenience for both parties (banks and the customers), the individual privacy Jordan is to a great extent threatened by the use of e-banking services.

In regards to e-banking, 17 of the 23 banks (or 73.9 per cent) provide a variety of products and services via electronic channels to their customers. These products and services range from basic e-banking service such as providing general information about the bank via online home page, to advanced e-banking activities such as: processing online application (for example, personal loans and car loans and credit card applications).

¹⁵⁵ *Central Bank of Jordan Law No 23 of 1971 (Jordan) Official Gazette*, No 2301, 25 May 1971.

¹⁵⁶ Article 1 of the *Payment System Regulations* [Arabic]: *Asool Gwaed Al Aamal wal Taleemat Al khasa Bel Magasa Al Electroonyh (Jordan)* avail <www.cbj.gov.jo>.

With respect to banks privacy policy/statement, the study shows that only 7 of the total 23 banks in Jordan (or 30 per cent) provide an online link to privacy policy/statement. For the local banks, only 4 banks (or 30 per cent) have a privacy policy or statement on their websites. The remaining three banks are foreign banks which they represent of 37.5 per cent of the foreign banks in Jordan. Surprisingly, the only two Islamic banks in Jordan do not have any privacy policy/statement on their websites even though both banks are providing e-banking products and services (0 per cent). The main requirement, however, of the Islamic banking operations is that the banks must be based on the *Shari'ah* (Islamic law). As noted above in Chapter Three, the *Shari'ah* considers the issue of privacy as a fundamental human right and it appears odd that in regard to privacy in the context of the Islamic e-banking there is no reference to the issue of privacy on their websites.

Many of the privacy concerns which arise in the e-banking context are the same as those arise in the e-government application (discussed in Chapter Four) which has been focused on the collection, use and disclosure of personal information. Additionally, there are two main concerns that can be identified regarding individual privacy in the context of e-banking in Jordan. These concerns (identified in the author's web-based survey) are (1) online privacy consent, and (2) transborder data flows. This is detailed in the next two sections. A case study on information practices of the foreign banks operating in Jordan then follows.

5.4.6.1 Online Privacy Consent

‘Online privacy consent’ is the agreement of an individual to the disclosure of his or her personal information to third parties when applying for e-banking products or services. Banks are required to obtain individual consent in order to collect, use, and/or disclose personal financial information.¹⁵⁷ The requirement for individual consent is significant as individuals then have the right to control their information and (depending upon the nature of the consent) to decide how the banks are to handle this information in what circumstances they are able to use it, (for example, credit check for offering/marketing further banking services, send greeting cards), and where and to whom they may disclose it (for example, mail out insurance products by the bank or associated company).

In order to examine this concern in the e-banking for Jordanian context, one of the most recognised banks, locally and internationally, in Jordan —the *Arab Bank* — has been selected to illustrate privacy issues associated with online personal consent.

The *Arab Bank* is the oldest — established in 1930 — and biggest bank in Jordan in terms of its assets.¹⁵⁸ The bank offers its customers many e-services, as is shown in the above Table. Customers can apply for credit cards online via the bank’s website. For the bank to process online credit card application, the following information must be submitted: full name, address, occupation, telephone numbers (land line or Mobile), nationality and current

¹⁵⁷ *Banking Law No 28 of 2000* (Jordan) art 44(b).

¹⁵⁸ Association of Banks in Jordan, ‘Development of the Jordanian Banking Sector (2000-2009), above n 26, 67.

income.¹⁵⁹ In order to grant the applicant credit, the bank needs to conduct a credit history check in order to approve the application. To conduct such a check the bank must disclose personal information about the applicant to other parties (for example, other banks, government agencies or credit reporting agencies). In order to be able to do so, the bank is required to obtain an agreement from the applicant that will allow the bank to disclose the applicant's personal information to these parties. However, on the online credit card application, there are no explicit or implicit terms that may make the applicant aware that his or her information may be disclosed to other parties in proceeding with the application. Although the *Privacy Statement* placed on the 'homepage' of the *Arab Bank* website notifies individuals that personal information provided by them may be used and disclosed for credit checks, this notification contains broader terms and is not an adequate substitute for such a notification being present on (for example) the actual credit card application form. Nor does it adequately substitute for a record of an individual's consent to the use/s (preferably clearly outlined) of the use of information there supplied.

In addition, the bank may change the terms and the conditions of the privacy statement at any time without prior notice. Subsequently, the bank may claim that the applicant has given his or her consent and rely on the privacy

¹⁵⁹ Arab Bank, *Apply Now* (2009) Arab Bank <<http://www.arabbank.com.jo/en/applynow.aspx>> at 21 October 2009.

statement on the 'homepage' website. With the absence of the relevant information on the application form itself, the individual is disadvantaged.¹⁶⁰

5.4.6.2 Transborder Data Flows (TDF)

Providing adequate protection of privacy is not a simple task in a country endorsing highly developed technologies in the banking sector. It becomes an even harder task to provide such protection on an international level due to some jurisdictional issues.¹⁶¹ In Jordan, one of the most noticeable recent features of the banking industry is its 'globalisation'. Jordan's commitment to WTO GATS obligations was an important factor in this. Full foreign ownership of banks in Jordan is now permitted. As of 30 December 2009, there were eight foreign banks in Jordan providing a variety of services and products.

While the benefits available to consumers in terms of low prices and more choices have resulted from the competition between the foreign banks and local banks, consumer privacy can be at a higher risk when transacting with foreign banks. This is simply because personal information can be transferred from one bank in Jordan, be stored in different bank or institution in different country, and be used by another bank or institution in a third country. The exchange of personal information from one country to another via the ICT channels such as computer network or telecommunications line is called the

¹⁶⁰ Appendix C, Exhibit 1, Arab Bank, *Privacy Policy* (2009) Arab Bank <<http://www.arabank.com.jo/en/privacypolicy.aspx>> at 21 October 2009.

¹⁶¹ Dan Jerker B Svantesson, 'Protecting Privacy on the "Borderless" Internet- Some thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168.

Transborder Data Flow (TDF).¹⁶² In the e-banking context, this exchange of personal information has become easier and faster due to the nature of the e-banking system which relies on the new technologies.

In order to examine the privacy implications of the TDF in Jordan carefully, this research will use the hypothetical example (below) to illustrate a number of the potential problems involved:

Faris is a Jordanian citizen and he is looking to buy a house in the capital Amman. He chooses to apply for home loan at HSBC Bank of Jordan. The application was submitted online through the e-banking services available by the HSBC Bank. The information required by the bank is: full name, telephone number, e-mail address, occupation, monthly income and other information related to the home loan. A few weeks later, Faris's application for the home loan was declined due to low income.

A few months later, the HSBC branch in Jordan had to terminate its operations due to the financial crisis. All customer data and applications were transferred and stored in the mainframe system controlled by the HSBC headquarters in London.

However, a year later, another financial institution based in Jordan contacted Faris and offered him a high interest personal loan (the high interest was to be charged due to his low income). Faris declined the offer as his income details has changed.

This hypothetical example is based on an analysis of the HSBC Bank's privacy policy located on the bank's website. The privacy policy reads: *'We may pass information about you and your dealings with us to other HSBC Group Companies or our agents to the extent allowed by law.'*¹⁶³ The example reveals that there are major concerns in regard to the privacy of Faris's personal information privacy in relation to TDF.

¹⁶² Regan, above n 62, 259.

¹⁶³ See Appendix C, Exhibit 15, HSBC, *Privacy and Security: Your Privacy Matters to Us* (2009) HSBC <http://www.hsbc.jo/1/2/ALL_SITE_PAGES/about-hsbc-jordan> at 23 October 2009.

First, Faris's personal information was able to be transferred and stored in different country; so Jordanian law may not be applicable to the transaction. Second, Faris would not be able to correct or amend his personal information stored by the foreign bank when his income details changed. Third, there are no guarantees for Faris that his information will be kept secure and confidential as it located in foreign country. Finally, Faris's personal information can be used by a third party based on the agreement with *HSBC Bank* in Jordan. The third party could be in Jordan or overseas.

5.4.7 The Privacy Implications of Foreign Banks in Jordan: A Case Study

The above concerns encouraged the author to further examine Jordan's foreign banks and their privacy information practices. Table 7 provides information obtained by an study of the online presence of all eight foreign banks operating in Jordan in relation to two types of business practices: (1) the sharing of personal information with third parties, and (2) the transfer of personal information outside Jordan. Each foreign bank received an evaluative code of: 'Certain 100%' or 'Uncertain 100%' for each type of practice. The use of such an evaluation is justified on the basis of a well-reasoned belief that the majority if not all of these banks collect personal information when offering e-banking services such as: credit cards online applications, internet banking, SMS, and so forth. However, this belief leads to the assumption that these banks share and transfer collected information. This assumption could not be confirmed as privacy policies/statements for a

number of foreign banks were inaccessible or unavailable. The study was carried out on 10 November 2009.

Only three of the eight foreign banks had privacy a policy/statement on their websites. As with regard to the first type of business practice (sharing personal information with third parties), the study found on the basis of their privacy statements/policies available online that these three banks do share personal information with third parties. These findings are ‘Certain 100%’. For the remaining five foreign banks, the study has found that these banks *may* share personal information with third parties; so the findings are ‘Uncertain 100%’ due to the lack of online information regarding their banking practices.

Table 7
Information Privacy Practices of Foreign Banks in Jordan

Bank Name & Website Address	Privacy Policy/Statement	Sharing Information With Third Party	Transfer of Information Outside Jordan
1.HSBC Bank Middle East www.jordan.hsbc.com	Yes	100% Certain	Uncertain 100%
2. Egyptian Arab Land Bank www.arakari.com.jo	No	Uncertain 100%	Uncertain 100%
3. Rafidain Bank www.rafidian-bank.org	No	Uncertain 100%	Uncertain 100%
4. Citibank N.A. www.citibank.com/jordan	Inactive	Uncertain 100%	Uncertain 100%
5. Standard Chartered Bank www.standardchartered.com	Yes	100% Certain	100% Certain
6. National Bank of Kuwait www.banqueaudi.com/jordan	Yes	100% Certain	Uncertain 100%
7. Audi Bank www.nbk.com	No	Uncertain 100%	Uncertain 100%
8. BLOM Bank www.blom.com/english	No	Uncertain 100%	Uncertain 100%

For the second type of business practice (the ability of banks to transfer personal information outside Jordan), the study found that, on the basis of its online policy statement, it is ‘Certain 100%’ just one bank in Jordan which

clearly states that personal information may be transferred to another country, and therefore no privacy protection is available for that information under Jordanian law once that information is abroad.¹⁶⁴ However, the author reasonably believes that the remaining seven foreign banks in Jordan *may* also transfer personal information to third parties outside Jordan, that is, that such a practice is possible. Given the lack of evidence on their websites, however, this finding is ‘Uncertain 100%’.

In summary, individual privacy in the banking industry of Jordan with regards to the e-services is yet to be protected and maintained. On the one hand, the adoption of the latest technologies makes it easier for banks to store, use and transfer large amount of personal information about individuals. On the other hand, at a time when there is no relevant law or regulation, individuals are unable to control their personal information when providing their information online (for example, when applying for a bank loan, credit card, and so forth). An individual’s right to control such information is important to protect and maintain their privacy.

The right for individual to control their personal information has become even more difficult when their information can be transferred outside Jordan. Currently, there is no law in Jordan to prevent personal information from being transmitted from foreign bank branches in Jordan to a main office located outside Jordan. Individuals are powerless and disadvantaged by not being able to make informed decisions when conducting online transactions

¹⁶⁴ Appendix C, Exhibit 18, Standard Chartered Bank Jordan, *Data Protection & Privacy Policy* (2009) Standard Chartered Bank Jordan <<http://www.standardchartered.com/jo/data-protection-privacy-policy/en/>> at 23 October 2009.

as the banks are in a far better position than the individuals in such matters due to a lack of appropriate legislation and regulation and, for example in relation to credit card or loan applications, the disproportionate power held by the bank (as credit provider) compared to most individual customers whose wealth does not afford them any particular attraction to the bank. It is worth noting that Jordan has no central agency to process complaints or disputes arising from banks/customer relationships.

The only available 'regulations' found with respect to individual privacy are those provisions included in the banks' privacy policies/statements which are located on the home page of the bank website. The intention of these policies is to increase consumer confidence in using e-services in the banking industry. However these policies/statements may not achieve this because of a lack of standardisation of expression and terms of statements of the banks' information practices and in the actual practices themselves. They also provide descriptive information of banks privacy practices rather than being legally binding codes. This weakness is further illustrated by the statistics included in Table 6 (above) which shows that only 17 of the 23 banks have privacy policies/statements.¹⁶⁵

5.5 Concluding Remarks

This chapter has presented a brief overview of Jordan's international trade obligations under multilateral and bilateral agreements including the WTO, JUSFTA and the J-EU Association Agreement. These obligations

¹⁶⁵ See Appendix C, Exhibits 1-20.

encouraged Jordan to adopt the free market approach, supported law reform, privatisation of public sector, and the provision of exemptions to foreign investments. However, within Jordan's new economy a threat to individual privacy can be identified. For example, a number of foreign entities in privatised sectors such as telecommunications and banking are permitted to transfer personal information to foreign countries. The question, here, is what is the protection available to this personal information?

The chapter has also focused on the issue of privacy for the private sector in Jordan. The telecommunications and banking sectors were selected for empirical examination in relation to privacy protection policies. For the telecommunications sector, the chapter has concluded that the protection of individual privacy is inadequate and insufficient for the current environment. As the empirical studies showed, most of the telecommunications companies in Jordan have the ability to collect, use, access and transfer personal information without the knowledge of the individuals supplying that information. It also showed that Jordan's telecommunication companies are under no legal obligations to inform individuals that their personal information may be transferred to other countries.

For the banking sector in Jordan, the chapter has provided an examination of all banks in Jordan in regards to their policies on privacy protection. The empirical study in this context showed that only 7 of the 23 banks in Jordan place a privacy policy/statement on their websites. With regard to foreign banks, only 3 of these 8 banks have anything to appearing on their websites

in regard to a privacy policy. The study has shown that while most banks in Jordan (17 of the 23 banks) provide electronic services and products through the ICT channels, less than 60 per cent of those with an online presence provide a privacy policy of statement.

The study on banks' information practices showed that online consent and transborder data flows are the most major issues to individual privacy. This is due to number of reasons. First, Jordan's new law on e-banking, the *Electronic Transactions Law No 85 of 2001* has no provisions to govern privacy protection when individuals are transacting via e-banking. Second, this law granted the Central Bank of Jordan the authority to regulate the e-banking, but up to the time of writing, there are no instructions from the CBJ on e-banking in general and no instructions regarding online privacy in particular, other than the banks themselves being able to formulate their own policies regarding electronic transaction as fits their own businesses. For example, there are no legal requirements for the banks to inform individuals that personal information obtained via e-banking transactions may be disclosed, or sold to a third party without their consent.

As regards transborder data flows (TDF), a study of Jordan's foreign banks showed that only one bank has provided a notice to individuals that their personal information may be transferred to other countries. This indicates that Jordan's foreign banks enjoy the freedom to transmit personal information about individuals outside Jordan. Such transfer increases the risks of privacy invasion. A third country — the recipient of such personal

information — may not have privacy protection laws to regulate the treatment of the information received.

The absence of applicable privacy laws on the telecommunications and banking sectors in Jordan and the right given to formulate their own policies has allowed companies in these sectors to adopt privacy policies/statement of their own devising and to place them on company's websites.¹⁶⁶ However, this chapter has shown that these policies/statements are inadequate and are unable address privacy concerns. And where they do exist, it is difficult for the average person to read them as they are often written in legal jargon. Even if customers could understand them, the amount of time required to read privacy policies is too great.¹⁶⁷ As the study also revealed, where they do exist such statements are often separated from the document or transaction page the user is accessing. Without an independent body (for example an ombudsman or authority) to which to appeal in regard to perceived privacy abuses (they cannot be breaches if legislation is non-existent), statistical evidence other than that presented above is difficult to assemble. But that here presented clearly reveals a lack of privacy provisions and therefore the possibility of abuses.

¹⁶⁶ See Appendix C, Exhibits 1-20.

¹⁶⁷ Joshua Gomez, Travis Pinnick and Ashkan Soltani, 'Know Privacy' (UC Berkeley, School of Information, 2009) 11.

Chapter Six

The Legal Landscape of Privacy Protection in Jordan

6.1 Introduction

The previous chapters have presented an overview discussion on privacy from different perspectives. Chapter Two provides discussion on the concept of privacy, and how it is difficult to provide a uniform definition of the concept of privacy. In Chapters Three and Four, individual privacy implications in the context of ICT in Jordan are examined and it is concluded that neither the public nor the private sector has adopted an effective mechanism for the protection of personal information.

This chapter looks at the current rules and legal principles under Jordanian law that address the issue of individual privacy. The intention of this chapter is to determine whether current laws and existing regulations are sufficient to protect and maintain individual privacy in Jordan. The Chapter first commences by briefly discussing the legal system in Jordan.

6.2 The Legal System in Jordan

It is worth mentioning that the legal system in Jordan is a civil law system. It is greatly influenced by the Code Napoléon, which was (as the name suggests) originally formulated in France in the wake of the French Revolutionary period which began in 1789 and culminated in the ascent to power of Napoléon Bonaparte in 1899. It was he who essentially thrust a new legal system upon the nation – the *Code civile des Français*, later more generally known as the *Code Napoléon* – a code based on an earlier 6th century

codification of Roman law. The Civil Code, the Civil Procedure Code, the Commercial Code, the Code of Criminal Procedure and the Penal Code are together known as the Napoleonic or the Code Napoléon.¹ In order to provide a better understanding of the legal system in Jordan, reference must be made to the Constitution of Jordan, the sources of the law and the court system of Jordan respectively.

6.2.1 The Constitution of Jordan

The modern history of Jordan goes back to 1921 when, with the help of the British government, the Emirate of Transjordan was established on the east bank of the Jordan River. In 1946, it achieved independence from Britain and was renamed the Hashemite Kingdom of Jordan.² The Jordanian constitution stipulates that the political system in the country is a constitutional hereditary monarchy.³

The Constitution calls for the separation of the executive, legislative and judicial branches. It gives the king several powers, including that of being the head of state,⁴ chief executive,⁵ and the commander in chief of the armed forces.⁶ Therefore, the king authorises the appointment and dismissal of the following: judges, the Council of Ministries, regional governors, and the mayor of the capital Amman. He also approves constitutional amendments,

¹ Catriona Cook et al, *Laying Down the Law* (5th ed, 2001) 5.

² Herbert M Kritzer (ed), *Legal Systems of the World: A Political, Social and Cultural Encyclopedia* (2002) 783.

³ *Constitution of the Hashemite Kingdom of Jordan, 8 January 1952* (Jordan), avail: <http://www.kinghussein.gov.jo/constitution_jo.html> at 2 February 2009.

⁴ *Ibid.*

⁵ *Ibid* art 31.

⁶ *Ibid* art 32.

grants special pardons, and, with the approval of the cabinet and the Parliament, declares war, concludes peace, and sign treaties and agreements.⁷

The Constitution also calls for the creation of a legislative branch of government, which consists of the Senate and the House of Representatives. The king appoints 60 senators, and the people directly elect the 120 members of the House of Representatives once every four years. Bills are first considered by the House of Representatives and then sent to the Senate for consideration. Any disagreement between the two houses over a Bill can be settled by a two-thirds majority vote in a joint session. Once a uniform Bill is passed, it is sent to the king, who can either approve it by a royal decree, or veto it and return it together with a statement of his reasons for doing so to the Lower House for reconsideration. By a two-thirds majority, the Parliament can override the king's veto.⁸

The two houses of Parliament enjoy equal status in several areas. These include their presence on several permanent committees, such as Legal, Financial, Administrative and Foreign Affairs. The Lower House representatives and the Senators also have parliamentary immunity from arrest while in office and freedom of expression during parliamentary deliberation. Despite these similarities, the Constitution gave special powers to the House of Representatives, including the questioning of the Cabinet or any individual minister on public policy. By a two-thirds majority, the House of Representatives may issue an official accusation against ministers and

⁷ Kritzer, above n 2, 784.

⁸ Ibid 785.

initiate investigation. They also have the exclusive powers of veto and of no confidence in the government or individual ministers.⁹

6.2.2 The Sources of Law in Jordan

The law of Jordan is based on — among other sources — a number of sources:

- (1) Legislation. This term refers to a set of legal rules (or Acts or amendments of Acts) made by the parliament to address new or existing issues that are a matter of a public concern.
- (2) Islamic Jurisprudence Rules (*Fiqh*). These rules are a set of opinions of distinguished Muslim scholars. These cover all aspects of religious, political and civil life, and include, for example, a number of areas such as: family law, inheritance, property and contracts. *Fiqh* also includes criminal law, constitutional law, and law regulating the administrative of the state and the conduct of war.¹⁰
- (3) The Principles of *Islamic Shari'ah* (Islamic law). The *Shari'ah* Principles are based — as discussed in Chapter Three — on the *Holy Qur'ān* and the *Sunnah* (the statements of Prophet Muhammad (pbuh) and constitute another primary source for settling disputes in Jordan. The *Shari'ah* governs matters concerning personal and family affairs, such as marriage, divorce, inheritance, child custody and wills for Jordanian Muslims.¹¹ Such disputes are settled through the religious courts, which are to be mentioned below.

⁹ Ibid.

¹⁰ Bogac A Ergene, *Judicial Practice: Institutions and Agents in the Islamic World* (2009) 19.

¹¹ Kritzer, above n 2, 785.

(4) *Customary Law (Urf)*. This is the oldest source of Jordanian law and is still observed in many parts of Jordan, particularly among the nomadic and semi-nomadic tribes. Customary law is based upon the customs of conciliation, arbitration, and family and clan honour, and offers the disputing parties the *Sulha* (settlement through conciliation) as a mechanism for settling interfamilial feuds, land disputes and personal injury outside the regular courts.¹²

The courts in Jordan must resolve any disputes and conflicts heard before them by applying the above sources respectively. In instances where there is no legal rule in the relevant legislation, the court must apply the rules of the Islamic jurisprudence (*Fiqh*). If the court could not find the applicable rule in the *Fiqh*, it must search within source of the Islamic *Shari'ah* principals (Islamic law) and apply the relevant rule. The last resort for the court is to apply the customary law or rules of justice.¹³

6.2.3 The Court System in Jordan

According to the Article 99 of the Constitution,¹⁴ the Jordanian legal system consists of three types of courts. These courts are:

1. The Religious Courts

The religious courts are divided into the *Shari'ah* courts and the tribunals of other religious communities. The *Shari'ah* courts have jurisdiction over

¹² Kritzer, above n 2, 785.

¹³ *Civil Code No 43 of 1976 (Jordan) [Arabic] Official Gazette* No 2645, 1 August 1976, art 2(2).

¹⁴ *Constitution of the Hashemite Kingdom of Jordan*.

matters regarding the personal status of Muslims,¹⁵ such as: marriage, divorce, wills and inheritance. The tribunals of religious communities are tribunals for those of those non-Muslim faiths that are recognised by the Government of Jordan. Appeals from the judgment of the religious courts are received by the courts of appeal. Jurisdictional conflicts between any two religious courts or between a religious court and a civil court are heard before a special court appointed by the Court of Cassation.¹⁶

2. The Civil Courts

The civil courts adjudicate any civil or criminal case not expressly reserved to the religious or special courts. There are four levels involved in civil jurisdiction: the magistrates courts, the courts of first instance, the courts of appeal and the Court of Cassation. In addition, the High Court of Justice was established to deal with administrative matters. Here below is a brief outline of these courts.

(1) The Magistrates Courts

These courts are established in accordance with the *Civil Courts Establishment Law* No 17 of 2001. Each consists of one judge¹⁷ who maintains jurisdiction over civil cases involving JOD 3000 or less and criminal cases involving a maximum term of imprisonment of two years or less.¹⁸

(2) The Courts of First Instance

¹⁵ Kenneth Robert Redden (ed), *The Legal System of Jordan*, Modern Legal Systems Cyclopedia (1990) 5.170.10.

¹⁶ Ibid 5.170.10-11.

¹⁷ *Civil Courts Establishment Law No 17 of 2001 (Jordan)* [Arabic] *Official Gazette* No 4480, 18 March 2001, 1308 art 3(b).

¹⁸ *Magistrate Courts Law No 15 of 1952 (Jordan)* [Arabic] *Official Gazette* No 1102, 1 January 1952, art 3 and 5.

These courts are established in accordance with Article 4 of the *Civil Courts Establishment Law* No 17 of 2001. Each consists of one judge in civil cases that are outside the jurisdiction of the magistrates courts. In criminal cases a court of first instance may consist of up to three judges if the penalty for the offence is the death penalty, life imprisonment or imprisonment for not less than 15 years.¹⁹

(3) *The Court of Appeal*

There are three courts of appeal in Jordan, with one located in each of three cities: Amman, Irbid and Ma'an. Each court is composed of at least three judges. The courts have jurisdiction over all civil and criminal cases which have been heard before a magistrate and first instance courts. A court of appeal may also have jurisdiction over cases where a specific law grants the court of appeal jurisdiction. All decisions of the court of appeal must be issued unanimously or be of majority status.²⁰

(4) *The Court of Cassation (Tamyiz)*

The Court of Cassation is located in the capital of Jordan, Amman. It consists of nine judges who sit in panels for 'exceptionally important cases'. The Court has jurisdiction over civil and criminal cases involving conflicting rulings by the three courts of appeal, or new constitutional questions, or are very complex cases, or cases that have public significance.²¹ The Court of Cassation has also jurisdiction over cases appealed from the religious courts, as well as cases involving any controversy between the Muslim and the

¹⁹ *Civil Courts Establishment Law No 17 of 2001 (Jordan)* [Arabic] *Official Gazette* No 4480, 18 March 2001, 1308, art 5.

²⁰ *Ibid* arts 6, 7 and 8.

²¹ *Ibid* arts 9 and 10.

Christian religious courts or tribunals.²² The decisions issued by the court must be unanimous or of majority status.

(5) The High Court of Justice

In accordance with Article 31 of the Jordanian Constitution, Law No 12 of 1992 was enacted to establish the High Court of Justice in Amman.²³ The Court consists of five judges who have jurisdiction over cases concerning disputes arising from the results of elections for municipal councils, or in relation to chambers of commerce, and industry and professional associations. The court also has jurisdiction over cases concerning: civil service employees who contest the fairness of appointments to civil service, conflicts over promotions, salary increases, transfers, forced retirements, and suspensions from work. It also considers cases from groups and individuals challenging the constitutionality of governmental laws and regulations, and cases involving appeals for the reversal of unlawful administrative regulations or the failure of an administrative unit to execute its responsibilities. The Court also has power to examine cases involving a conflict with the Constitution, misapplication and misinterpretation of the law, and abuse of power or office.²⁴

3. The Special Courts

The special courts are to be established in accordance with Article 99 of the Constitution. The special courts include the following types of courts:

²² Ibid art 11.

²³ *High Court of Justice No 12 of 1992 (Jordan) [Arabic] Official Gazette No 3813, 25 March 1992, 516*

²⁴ Ibid art 9.

(1) *The Court of Serious Crimes*²⁵

The court consists of three judges and a prosecutor. The special court has jurisdiction over serious crimes involving murder, rape, and kidnapping. The cassation court automatically reviews any rulings of the court that involve the death penalty and jail sentences of more than five years.²⁶

(2) *The State Security Court*²⁷

The court consists of a panel of three military and/or civilian judges²⁸ and has exclusive jurisdiction to try members of the military and civilians who are charged with armed insurrection, drug trafficking, spying, or crimes against the armed forces, the police, the ministries, and members of the royal family. The law gives the prime minister power to establish security courts in response to special circumstances as required in the interests of the public or in response to a request by the commander of the armed forces.²⁹ The law also stipulates that the state security courts' rulings can be appealed to the Court of Cassation, and that rulings involving the death penalty must be reviewed by that court.³⁰

(3) *The Military Courts*

The military courts consist of military judges and prosecutors. They have jurisdiction over cases involving only military personnel. They have the authority to try the officers of the armed forces, students of the military

²⁵ *Court of Serious Crimes Law No 19 of 1986 (Jordan) [Arabic] Official Gazette No 3380, 16 March 1986, 457*

²⁶ *Ibid* arts 3 and 4.

²⁷ *State Security Court Law No 17 of 1959, (Jordan) [Arabic] Official Gazette No 1429, 1 July 1959, 529.*

²⁸ *Ibid* art 2.

²⁹ *Ibid* art 3.

³⁰ *Ibid* art 9.

institutions and schools, prisoners of war, and military officers of any foreign army located in Jordan.

(4) *The Police Courts*

The police courts have jurisdiction over crimes committed by police officers of all levels. A police court consists of three judges and the public prosecutor of the police. The procedures of the court are to be in accordance with the Code of Criminal Procedures. The rulings of the police court can be appealed to the Court of Cassation.

(5) *The Municipal Courts*

The establishment of municipal courts is based on special regulations in accordance with the *Municipal Court Establishment Law No 72 of 2001*.³¹ These courts are considered to be equal to the magistrates courts. A municipal court has jurisdiction over minor cases that occur within the borders of a municipality.

Additionally, there are a number of special courts established by the legislative branch complete the court system in Jordan. These courts are: the Income Tax Court, the Customs Court, and the Land and Water Courts. There are also special courts that have the specific jurisdiction of interpreting the Constitution and the laws of Jordan. The High Tribunal interprets the Constitution at the request of the Prime Minister or of either chamber of the National Assembly, while the Special Council has the

³¹ *Municipal Courts Establishment Law No 72 of 2001 (Jordan) [Arabic] Official Gazette No 4520, 2 December 2001, 5567.*

jurisdiction to clarify and provide interpretation on a specific matter of law which has never been decided by any of the above courts.

6.3 Laws Applicable to Privacy Protection in Jordan

Unlike the US and the EU, Jordan has no specific law and/or regulation to address the violations of individual privacy. However, individuals may rely on a number of laws to protect their privacy. This section examines the laws most applicable to privacy protection in Jordan. These laws are divided into three areas:

- (1) major laws including: the *Constitution of Jordan*, the *National Centre for Human Rights Law* No 50 of 2006, the *Civil Law* No 43 of 1976, the *Penal Code* of 1960 and the *Law on Guaranteeing the Right of Access to Information* No 47 of 2007;
- (2) Telecommunications privacy laws, namely: *Telecommunications Law* No 13 of 1996, and *Postal Service Law* No 34 of 2007; and
- (3) Financial privacy laws, namely: *Banking law* No 28 of 2000, *Credit Information Law* No 15 of 2010, and *Anti-Money Laundering Law* No 46 of 2007 (and its regulations).

These laws will be examined in detail below.

6.3.1 Major Laws³²

6.3.1.1 The Jordanian Constitution and Privacy

The second chapter of the *Jordanian Constitution*³³ contains provisions recognising the rights and duties of the Jordanian people. The Constitution specifically guarantees that:

Jordanians shall be equal before the law. There shall be no discrimination between them as regards to their rights and duties on grounds of race, language, or religion'.³⁴

Further, the Constitution states that 'personal freedom shall be guaranteed,'³⁵ and that 'no person [is] to be detained or imprisoned except in accordance with the provisions of the law'.³⁶ It also provides that the 'state shall safeguard the free exercise of all forms of worship and religious rites in accordance with the customs observed in the Kingdom, unless such is inconsistent with public order or morality'.³⁷

Furthermore, the Constitution specifically guarantees Jordanians the freedom of opinion; it states that 'every Jordanian shall be free to express his opinion by speech, in writing, or by means of photographic representation and other forms of expression, provided that such does not violate the law'.³⁸

The Constitution also declares that Jordanians have the rights to hold

³² The selection of these laws is significant for any discussion on the issue of privacy. For this reason these laws are categorised as 'major'.

³³ *Constitution of the Hashemite Kingdom of Jordan*.

³⁴ *Ibid* art 6.

³⁵ *Ibid* art 7.

³⁶ *Ibid* art 8.

³⁷ *Ibid* art 14.

³⁸ *Ibid* art 15(1).

meetings' and 'establish societies and political parties' in accordance with the law.³⁹

With respect to individual privacy, the Jordanian Constitution has no explicit mention of the term 'right to privacy' of individuals, but rather contains some provisions that are broadly relevant to the concept of privacy. These provisions are only applicable in specific situations. For example, Article 10 of the Jordanian Constitution stipulates that 'Dwelling houses shall be inviolable and shall not be entered except in the circumstances and the manner prescribed by law.'⁴⁰

This Article can be traced back to the *Shar'iah* that is the foundation of Jordanian law. As noted above in Chapter Three, the two main sources of Islamic law: the *Holy Qur'an* and the *Sunnah* have explicitly recognised the sanctity of the right to privacy in the residential context.

The author believes that this article only provide protection to individuals at the time when there is a physical intrusion to their homes without proper cause. However, individuals may not be able to rely on this article to protect their privacy if forms of home intrusions other than physical have been undertaken. For example, an enforcement agency (such as the police) may legally (that is, with a warrant) enter a person's house to carry out a physical search and, using hiding electronic devices such as a camera, obtain images within the house without the person's consent. The affected person may not

³⁹ Ibid art 16(1)(2).

⁴⁰ Ibid art 10.

rely on Article 10 of the Constitution as the physical search of house has been conducted in accordance with the law. In another example, an individual may not claim that his/her home has been intruded upon — in contravention of this article — when a telemarketing company using a telephone solicitation collects his/her personal information without obtaining their consent.

It is believed that both activities in the above examples (taking images via camera and collecting personal information via phones without consent) are forms of home intrusions and therefore violate the right of individual privacy; however, Article 10 may not be sufficient to protect and maintain this right.

The second article which is relevant to the right of privacy is Article 18 of the Jordanian Constitution. It stipulates that: ‘All postal, telegraphic communications shall be treated as secret and as such shall not be subject to censorship or suspension except in circumstances prescribed by law.’⁴¹

A number of comments can be noted concerning the above article. First, the author believes that the Jordanian constitution should use the term ‘private’ rather than ‘secret’. Although there are some similarities between ‘privacy’ and ‘secrecy’, the difference, however, is well noticed. ‘Privacy’ is viewed as a right, but ‘secrecy’ is considered as a choice. For example, two persons are expected to have a private conversation when the need arises, while secrecy can be viewed as dark, embarrassing, even dirty. Furthermore, a secret is

⁴¹ Ibid art 18.

shared willingly by one party and told to another or kept inside for a lifetime; privacy is an expectation. In a simple word, privacy is an expectation that individuals have when it is appropriate; secrecy is the act of hiding something from one person, the world at large or oneself. For example, marital sexual relations, the contents of a handwritten diary or of the hard drive of a computer may be protected. Conversely, illegal sexual activities, a handwritten diary detailing armed robberies, or paedophilic pornography must be concealed as 'secrets'.⁴² The key difference appears to be the legality of the activity being undertaken or recorded, and the desirability of the release of relevant information regarding that activity. Privacy concerns the activities of a person or persons where such activities or information is not in breach of any legislation, that is, while it may be of interest to the person concerned and the release of information pertaining to that activity to the wider community may satisfy prurient interest, it is not 'in the interest' of the persons concerned nor in the interest of the wider community for the activity or information to be made publicly available. Hence the word 'private' may constitute a more accurate translation of the concept involved.

Second, the article only includes postal and telegraphic communications under its protection. A narrow interpretation of this article would establish that other forms of communications such electronic mail may not be protected under this article.

⁴² William G Staples (ed), *Encyclopedia of Privacy* (2007) vol 2, 483.

Third, a government agency may intercept private communications when a specific law permits it to do so. For example, the Electronic Warfare Unit (EWU) within the Armed Forces of Jordan is using electronic devices to intercept citizens' telephone conversations for the purpose of protecting national security and/or discovering illegal activities.⁴³ The argument remains open, however, on the subject of whether the 'private matters' disclosed by intercepting such communications are protected under this constitutional article.

6.3.1.2 The National Centre for Human Rights Law No 51 of 2006

The National Centre for Human Rights (NCHR) in Jordan was established in 2002 by virtue of temporary law No 75 and became a permanent law No 51 in 2006.⁴⁴ There are three main objectives of the establishment of the Centre: (1) to protect and enhance the situation of human rights and public freedoms in Jordan; (2) to promote the principles of human rights within the Kingdom by drawing from the tolerant teaching of Islam and the heritage of Arab Islamic values as well as the rights enshrined in the Constitution and the principles enshrined in international charters and covenants; (3) to support the democratic process within the Kingdom in order to create a comprehensive and balanced model based on protecting freedom, safeguarding political pluralism, respecting the rule of law and guaranteeing the right to economic, social and cultural development; and (4) to develop

⁴³ For security and confidential reasons, the sources and names within the EWU cannot be cited at this time.

⁴⁴ *National Centre for Human Rights Law No 51 of 2006, (Jordan) Official Gazette No 4787, 16 October 2006, 4026.*

national legislation related to human rights in the line with international agreements and standards to which Jordan is committed.⁴⁵

The NCHR is an independent national agency. It has a juridical personality with full financial and administrative independence from government control. It is authorised to conduct various tasks related to human rights issues in Jordan. In its 2008 annual report, the NCHR addressed the state of human rights in Jordan. The report provides a comprehensive evaluation of civil, political, economic, social and cultural rights. Citing the legal framework in Jordan, the report deals with each human right separately, and seeks to determine the extent to which Jordan complies with the international instruments that the country has ratified.⁴⁶ While the NCHR report addresses 27 human rights-related issues, the right to privacy was not mentioned in the report.⁴⁷ This means that the right to privacy has been disregarded, and perhaps is not very well protected in the country. The fact that the concept of the 'right to privacy' is yet to be legally, socially or culturally recognised in Jordan may result from the lack of awareness and knowledge of such right within the society.

6.3.1.3 The Civil Code No 43 of 1976

The *Civil Code* No 43 of 1976⁴⁸ provides comprehensive regulations for all civil matters, including personal rights, contracts, property rights, mortgage

⁴⁵ Ibid art 4.

⁴⁶ National Centre for Human Rights, 'State of Human Rights in the Hashemite Kingdom of Jordan (2008)' (National Centre for Human Rights, 2008) 6, <http://www.nchr.org.jo/uploads/NCHR-2008_Report-Final-Eng.doc>.

⁴⁷ Ibid.

⁴⁸ *Civil Code No 43 of 1976 (Jordan)* [Arabic] *Official Gazette* No 2645, 1 August 1976.

and ownership rights. With respect to the right to privacy, the Code has no explicit reference to this right, neither in the personal rights section, nor in any other section of the Code. The only texts that may be relevant to the right to privacy are those of tort law stipulated under Articles 47, 48, 49, 256 and 267(1).

Article 47 states that: 'No one can surrender his/her personal freedom.' Under Article 48, '[E]very person has the right to stop unlawful violation of his/her natural personal rights and shall seek compensation for any damages incurred as a result.' In addition, Article 49 goes further to protect a person's name and/or pseudonym if it is unlawfully used by someone else. The injured person has the right to stop the violation of their right to their name and/or pseudonym and may seek compensations for any damages incurred as a result of this violation.⁴⁹

In spite of the fact that the Civil Code does not elaborate as to what are the 'natural personal rights', it is the author's interpretation that these rights may cover the right to privacy. This interpretation is based on Article 2(1) of the Code, which provides sequential steps for interpretation of the provisions of the law. First, in construing the *Civil Code*, the courts are required to look at the rule of the Islamic Jurisprudence (*Fiqh*). If such rules cannot be found, the second step is to look at the principals of *Shari'ah*. As mentioned in Chapter Two, both Islamic Jurisprudence and *Shari'ah* regarded the right to privacy as a natural personal right rather than a property right.

⁴⁹ Ibid art 49.

Furthermore, the *Civil Code* provides a general rule to address tortuous acts. Article 256 provides that every wrongful act or omission committed against another person must be compensated by the tortfeasor.⁵⁰ This Article is mainly concerned with providing compensation for personal injuries and property damage caused, negligently or intentionally. This Article may also apply to other interests such as personal freedom, honour, and reputation, and therefore, require remedies. Article 267(1) provides that compensation shall be provided for wrongful acts against someone's personal freedom, honour, reputation, social position and/or financial position.⁵¹ The protection of someone's reputation is also protected under the Jordanian *Penal Code*, as will be discussed in detail below.

Due to the similarity between privacy and reputation, and the close relationship that may exist between the two, the author believes that the application of Article 267(1) may be extended to include the right to privacy.

As claimed in Chapter Two (when discussing international human rights instruments), the attack on someone's honour and reputation is an attack on his/her right to privacy. Therefore, it can be concluded that the Civil Code in Jordan would provide some legal protection to the right to privacy. However, this legal protection may not be sufficient and adequate in other situations. For example, the misuse of someone's personal information cannot be categorised as an attack on his/her reputation and, therefore, the injured person cannot rely on the above Article.

⁵⁰ Ibid art 256.

⁵¹ *Civil Code No 43 of 1976 (Jordan) [Arabic] Official Gazette No 2645*, 1 August 1976, art 267(1).

6.3.1.4 The Penal Code No 16 of 1960

The *Penal Code* No 16 of 1960⁵² of Jordan has many provisions where the Code protects personal reputation that may be used to protect privacy. The *Penal Code* prohibits three types of acts: libel, slander and contempt.

Libel involves the spreading or communication of material — even in the form of questions or the expression of mere suspicions — that could cause harmful consequences to a person’s honour and dignity or may place this person in a very low class within the society without any justification.⁵³ In this context, information dissemination or publication may take a number of forms, including newspaper and magazine articles, television and radio broadcasts, cartoons, paintings, photographs, posters or any other type of publication, which includes on the internet or transmission of text, photo or filmed material via a mobile phone.⁵⁴

Slander means an act of oral communication that causes harmful effects to a person’s honour, dignity and reputation. Personal reputation can be harmed by someone else in an oral communication — verbally by utterance to another either directly or by telephone or communicated over conference calls or conversations conducted utilising various forms of computer technology (such as ‘Skype’) — even without written or broadcast publication (in such forms as listed further above, for example). Again such

⁵² *Penal Code No 16 of 1960, (Jordan) [Arabic] Official Gazette No 1487, 1 January 1960.*

⁵³ *Ibid* art 188(1).

⁵⁴ *Ibid* art 189(3)(a)(b) and (4)(a)(b).

communication can take the form of a question or questions being asked, or a suspicion or suspicions being aired.⁵⁵

The third type of protection afforded reputation is the tort of contempt. Contempt means every insult — other than libel or slander — directed *at the plaintiff*, in forms such as writing, telephone conversation or telegraphic record, physical action, and/or face to face conversation.⁵⁶

Under the Jordanian Penal Code, the defendant will still be liable for defamation action even if the statement is true, with the sole exception being in the case where the information is true and related to the plaintiff's public position. This exception is justified on the ground that the revelation of information would benefit the society as a whole.

The author believes that the above are the torts most relevant to privacy protection, particularly in the context of informational privacy. The law concerning the defamation rules has, however, been taken to an extreme to protect individual privacy when it states that a defendant could be liable for defamation even where there is no explicit reference to the name of the plaintiff. In a 1996 case, the Cassation Court of Jordan (the highest court in the Jordanian legal system) decided that, in accordance with Article 188(3) of the *Penal Code*, the explicit naming of the plaintiff is not required in order to prove a defamation case.⁵⁷

⁵⁵ Ibid art 188(2).

⁵⁶ Ibid art 190.

⁵⁷ The Court of Cassation, Case No 636 of 1996, 003950 (Criminal Case) [Arabic] avail <www.lob.gov.jo> at 26 March 2009.

Furthermore, Article 366 of the Code grants the relatives of a deceased person the ability to protect him/her from acts of libel and slander directed at their deceased person.⁵⁸ The *Penal Code* also criminalises acts against personal freedom and honour. Article 346(1) of the Code protects persons from being held unlawfully or without legitimate reasons.⁵⁹ While Article 347(1) protects the privacy of one's home from unauthorised entry, Sub-section (2) of the same article provides harsher punishment if the act occurred at night, involved the use of violence against the owners of the house or the use of tools or weapons to break into the house.⁶⁰

Despite the fact that the above provisions of the *Penal Code* protect individuals from bodily harm, and from damage to their honour and reputation, it does not provide adequate protection in terms of a sufficient remedy when their privacy is violated. For example, using a mobile phone to take photographic images of a naked woman was considered by the court as a sexual assault, despite there having been no physical contact between the victim and the offender.⁶¹ If the court had decided that the offence committed had been a violation of her privacy, the court would not have been able to apply the *Penal Code* provisions as there are no such provisions to deal with such matters.

⁵⁸ *Penal Code No 16 of 1960 (Jordan) [Arabic] Official Gazette No 1487*, 1 January 1960, art 366.

⁵⁹ *Ibid* art 346(1).

⁶⁰ *Ibid* art 346(1).

⁶¹ Gerasa News, *Convicted Offenders on Sexual Assault Charges: Taking Images of Minor's Underwear by a Mobile Phone [Arabic]* (2011) Gerasa News <<http://www.gerasanews.com/web/print.php?a=39651>> at 4 January 2011.

6.3.1.5 The Law on Guaranteeing the Right of Access to Information No 47 of 2007

The *Law on Guaranteeing the Right of Access to Information* was enacted in 2007 in an attempt to make governmental information accessible to any citizen who requests such information (such a law may be known in other countries as ‘freedom of information’ legislation). The law is an important step towards an effective and transparent democracy by allowing the public to participate in the decision-making process. It is also a significant piece of legislation that helps to reveal fraud, corruption and incidents where public resources are wasted.

Another reason for the importance of this law is that it is the first piece of legislation to provide a clear definition to the term of ‘information’. Article 2 defines all types of data, records, statistics, or any documents that are written or unwritten, recorded, pictured or electronically saved as ‘information’.⁶² This definition may help to provide a definition of personal information not just to the public sector but also for the private sector.

At first glance, from the above a person may, logically, assume that there is a privacy law in Jordan to protect information from disclosure; and, therefore, in order to accommodate an exception, the enactment of Law No 47 of 2007 was required to allow the access to information. However, this is not the case in Jordan — the country lacks specific privacy legislation. It is odd that the legal system in Jordan guarantees citizens their right to access to

⁶² *Law on Guaranteeing the Right of Access to Information No 47 of 2007 (Jordan) [Arabic] Official Gazette No 4831, 17 June 2007, 4142, art 2.*

information but it does not have a 'law' to protect their information (that is, the right to privacy). Therefore, it is important to examine whether or not the Law No 47 of 2007 protects individual privacy within its provisions.

In order to obtain governmental information under this law, the requester must complete the designated form and submit it to the Information Council, which has been established in accordance with this law and whose main responsibility is to provide the information requested.⁶³ The person making the request has to determine clearly the type of information he/she requesting and from which government agency the information is to be requested. The government agency must respond within 30 days, indicating whether or not it will provide the information requested, and if not, the reasons why.⁶⁴ In case of rejection, the requester may file a complaint with the agency asking it to reconsider its decision. If dissatisfied with the result, the requester has the right to appeal to the High Court of Justice to enforce his or her rights.⁶⁵

The government agency, however, may denied the requester his or her request if the information requested comprises or contains (1) secrets and classified documents protected by another law; and/or (2) classified national defence or foreign policy information; or is (3) related only to government agency rules and practices; or comprises (4) confidential business information, such as trade secrets, and commercial or financial information;

⁶³ Ibid art 3.

⁶⁴ Ibid art 9.

⁶⁵ Ibid art 17.

or (5) law enforcement records, such as information from initial investigations.⁶⁶

Despite the fact that Jordan lacks specific privacy laws and/or regulations, the author believes that the *Law on Guaranteeing the Right to Access to Information of 2007* has two distinct exemptions that may provide a legal framework to privacy protection in Jordan. First, Article 10 of this law prohibits persons from requesting information that may include discriminative data (that is data that may be used as a basis of unwarranted discrimination) such as: religious affiliation, ethnicity or race, gender and skin colouring.⁶⁷ Second, the law protects personal privacy in government records where disclosure would constitute a clearly unwarranted invasion of personal privacy. It prohibits government agencies from providing information that includes personal educational records, medical records, employment records, bank accounts and transactions, professional secrets and personal telecommunications information.⁶⁸

In sum, a number of shortcomings can be noted on this law. First, the general rule of Law No 47 of 2007 is that it requires government agencies to disclose information rather than requiring the agency to have a policy of nondisclosure. The provisions concerning privacy merely provide grounds for government agencies to refuse to disclose information if they so choose. The government agencies will have the right to decide whether or not to

⁶⁶ Ibid art 13.

⁶⁷ Ibid art 10.

⁶⁸ Ibid art 13(6) and (7).

disclose information to the requester. Second, the privacy provisions included in this law do not specify the amount of personal information to be released and whether or not a third party can use such information after the initial release. Finally, the current law does not clearly establish the hierarchy between the individual's privacy interest and the public interest. For example, if a disclosure of personal information violates individual privacy, but protects public interest, which interest is it that the law is required to protect?

6.3.2 Privacy Laws Concerning Jordan's Telecommunications Sector

As has been noted above — in Chapter Five — there have been substantial changes to the telecommunications sector in Jordan. These changes aim to liberalise, privatise and create a fair and competitive market concerning telecommunications. This section examines whether or not the Jordanian legal system includes privacy laws and/or regulations that may be applicable to protect individual privacy. In relation to this matter, the most relevant laws to be examined are the *Telecommunications Law* No 13 of 1995 and the *Postal Services Law* No 34 of 2007 respectively.

6.3.2.1 The Telecommunications Law No 13 of 1995⁶⁹

This law regulates the activities of a number of actors in the telecommunications and information technology sector in Jordan. Chapter I of this law provides a number of definitions for a range of frequently used but

⁶⁹ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002 (Jordan) Official Gazette* No 4416, 17 February 2000. The original law was issued in the *Official Gazette* No 4072, 1 October 1995

often technological and/or complex terms, such as: ‘telecommunications’, ‘telecommunications service’, ‘information technology’, ‘radio waves’, ‘radio communication’, ‘radio frequencies’, ‘beneficiary’ and ‘licensee’.⁷⁰ However, one major criticism of the law with regard to personal privacy is that the law does not provide a definition to the term of ‘personal information’. Much of the telecommunications service providers’ activities depend on the processing of personal information. An inadequate definition of what is meant by the term ‘personal information’ or the failure to define the term at all (as is the case in this instance) means that telecommunications service providers are able to obtain whatever information they desire. Personal information can be either relevant to the provision of telecommunications services (such as customer name, address, contact details, profession) or irrelevant to such service provision (for example, marital status, health status or history, income and other financial details).

However, the *Telecommunications Law of 1995* has a number of provisions concerning individual privacy protection in the telecommunications context.

Article 71 of this law makes it an offence to spread, disclose, or record the

⁷⁰ Art 2 of the law provide definition to number of complex terms such as: (1) ‘Telecommunications’ which is defined as: ‘any conveyance, emission, reception, or transmission of signs, signals, sounds, images or data of any nature by means of wire, radio, photic of any other means of electronic system’; (2) ‘Information Technology ... the generation, manipulation and storage of information using electronic means’; (3) ‘Radio Communications ... the transmission by radio of text, signs, signals, images, or sounds of all kinds, including all instrumentalities, facilities, apparatuses, and transmission associated services such as the transmission, reception, conveyance of communications’; (4) ‘Beneficiary ... a person who benefits from public telecommunications services using telecommunications means’; (5) ‘Licensee’ ... a person who has acquired a license in accordance with the provisions with the law’; and (6) ‘Public Telecommunications Service ... a telecommunications service provided for compensation to the beneficiaries in general or a certain category thereof in accordance with this law’.

contents of any communication without legal justification.⁷¹ Despite the fact the law does not define the term ‘communications’, it is the author’s understanding that ‘communications’ may mean both ‘telecommunications’ and ‘radio communications’ as defined in Article 2 of this law.

Article 76 of the *Telecommunications Law of 1995* makes it an offence to intercept, obstruct, alter or strike out the contents of a message carried by the telecommunications networks.⁷² It is unclear, however, whether or not this article prohibits the access to messages by an employee of a network in the performance of his or her duties. An employee of a network appears to be able lawfully to access or ‘intercept’ stored information as part of his or her employment,⁷³ but such access is permissible only insofar as such access is required by their duties and therefore not otherwise.⁷⁴

Furthermore, Article 77 makes it an offence to withhold a message, or refuse to transmit messages, or make copies, or reveal a message, or tamper with the information related to any subscribers, including unpublished telephone numbers and sent or received messages.⁷⁵

The author believes that there are a number of issues that would make the above provisions insufficient in relation to individual privacy in the telecommunications sector in Jordan. First, with respect to Article 71, the

⁷¹ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002 (Jordan) Official Gazette* No 4416, 17 February 2000. The original law was issued in the *Official Gazette* No 4072, 1 October 1995, art 71.

⁷² *Ibid* art 76.

⁷³ *Ibid* art 65(a).

⁷⁴ *Ibid* art 65(b).

⁷⁵ *Ibid* art 77.

legislator should have included 'to use the information' instead of 'to spread the content'. The phrase 'spread the content' may, in the absence of a definition, appear to require that the general public must know of the content in order for the action to constitute an offence under this Article, while the use of the phrase 'to use the information' may enable such use to constitute a violation of personal privacy even though the use occurred without the knowledge of the general public. Second, with respect to Articles 76 and 77, the author may argue that these may only apply to the content of 'messages' rather the content of the communications in general. Other forms of communications (such as: visual images transmitted online, Skype calls as opposed to written emails, stored images as attachments) may not be subject to Articles 76 and 77.

Third, this law grants the staff of the Telecommunications Regulatory Commission (TRC) the right to intercept any communications in Jordan, regardless of whether other legislation would consider such an action as a breach of the confidentiality or a violation of the integrity of communications.⁷⁶ However, the law makes it an offence for the TRC staff to spread or publicise any of the intercepted communications or their content.⁷⁷

This issue presents a significant gap in the *Telecommunications Law* in regard to privacy protection. The author's view is that a warrant authorising access or interception of information must be obtained. It is also important to set

⁷⁶ Ibid art 65(a).

⁷⁷ Ibid art 65(b).

out a warrant process that determines which staff and agencies are allowed to access stored communications.

6.3.2.2 The Postal Services Law No 34 of 2007⁷⁸

The *Postal Services Law of 2007* grants the TRC the authority to regulate and monitor the activities provided by the postal service operators. The TRC has also the authority to set the guidelines for the public and the private postal operators.⁷⁹ Accordingly, the law has considered the following activities as postal services: (1) receiving and delivering letters and post cards, and parcels, (2) local and international money orders, and (3) the operation of private mail boxes.⁸⁰

The only provisions that are relevant to privacy are those stated in Article 24 of this law. It makes an offence (punishable by up to three years imprisonment or a fine by up to JOD 1000 or both) for public or private personnel to disclose classified information about his/her occupation, or disclose information about the contents of postal services unless such a request is permitted by the law (for example, a request by customs officers, police, and so forth).⁸¹ However, one major criticism of the law is that it does not have privacy provisions to protect the use personal information when using a postal service. For example, if a person (for convenience's sake here referred to as 'Faris') wants to use the postal money transfer service to transfer money from Jordan to another country, he must submit some

⁷⁸ *Postal Services Law No 34 of 2007 (Jordan) [Arabic] Official Gazette No 4823, 1 May 2007, 2645.*

⁷⁹ *Ibid* art 9.

⁸⁰ *Ibid* art 11.

⁸¹ *Ibid* art 24.

personal information (name, address, contact details, and banking details (which may include credit card details) to the postal operator in order for the operator to deliver this service in accordance with the law. The law only guarantees to protect the postal service itself which includes: the money, the transfer, issuing of receipts and the confirmation of transfer. Therefore, the issue in question here is whether or not Faris's personal information can be processed by the postal service provider and/or a third party?

The 'process' refers to the use, disclosure, access and transfer of personal information. In this context, the author believes that the Postal Services Law No 34 of 2007 should be amended to include provisions that explicitly regulate the treatment of personal information.

6.3.3 Privacy Laws Concerning the Banking Sector in Jordan

'Financial privacy' means that banking records and financial information about individuals are not to be shared with outside parties without their consent. In Jordan, financial privacy could be threatened as a result of the advances of the new technologies which have enhanced the ability to collect, use and disclose vast amounts of financial information about individuals. While privacy implications in the banking context were discussed in Chapter Five, this section examines any applicable laws and/or regulations in the financial sector. Again, the intention of such an examination is to ascertain whether or not these laws and/or regulations provide sufficient financial privacy protection.

6.3.3.1 The Banking Law No 28 of 2000⁸²

The *Banking Law* No 28 of 2000, as amended in 2003, regulates in — Articles 72, 73, 74 and 75 — ‘banking confidentiality’ with respect to an individual’s bank records under legal liability. Article 72 of the law provides that:⁸³

A bank shall observe full confidentiality regarding all accounts, deposits, trusts, and safe-deposit boxes of its customers. It shall be prohibited from providing directly or indirectly any information thereon except upon a written consent of the owner of such account, deposit, trust, or the safe-deposit box, or an heir of his, upon a decision issued by a competent judicial authority in a current litigation, or due to one of the permissible situations pursuant to the provisions of this law. This prohibition shall remain in effect even if the relationship between the bank and the client has terminated for any reason whatsoever.

The author’s view on the prohibition included in the above Article is that the term ‘full confidentiality’ does not grant individuals a ‘right’ to financial privacy. It is believed that the prohibition is to protect the interests of both parties, that is, the banks and their clients. The distinction between ‘privacy’ and ‘confidentiality’, as discussed in Chapter Two, is a very fine one. The concept of ‘confidential’ refers to situations in which the first party (the client) has entrusted information to other (second) party (the bank) on the assumption that there will not be any unauthorised disclosure of the first party’s information. Privacy, however, is a much broader concept than confidentiality, because it entails restrictions on a number of practices related

⁸² *Banking Law* No 28 of 2000 (Jordan) *Official Gazette* No 4448, 1 August 2000, 2950.

⁸³ *Ibid* art 72.

to the treatment of personal financial information, including its collection, use, access, and disclosure.

Article 73 prevents bank employees from disclosing clients' bank records without legal justifications. It states:⁸⁴

All present and former administrators of the bank shall be prohibited from providing any information or data on the clients or their accounts, deposits, trusts, safe-deposit boxes, or any of their transactions, or disclosing or enabling others to have access to such information and data in situations other than those permitted under this law. Such prohibition shall apply to anyone who by virtue of his profession, position or work, directly or indirectly, may have access to such information and data, including employees of the Central Bank and auditors.

The protection of the bank records provided by the above Articles is only available to those who have records with the bank including: accounts, deposits or trusts and safe-deposits boxes. This protection, however, does not extend to include financial information provided to the bank by individuals who do not have any dealings or ongoing relationship with the bank. For example, if Faris wishes to transfer an amount of money to a person or institution outside Jordan by using the service provided by Bank A, Article 72 of this law may be irrelevant to the confidentiality or otherwise of the information supplied by Faris for the transfer to occur. This is simply because Faris is not a client and does not have financial records with Bank A.

The *Banking Law of 2002* also has a number of exceptions concerning the 'confidentiality' of the financial information. According to Article 74 of this

⁸⁴ Ibid art 73.

law, there are certain circumstances which allow the banks in Jordan to disclose financial information about their clients. These circumstances are:⁸⁵

- (a) The duties provided in law to be performed by the auditors appointed by the general assembly of a bank or by the Central Bank pursuant to the provisions of this law.
- (b) The tasks and measures undertaken by the Central Bank pursuant to this law or the Central Bank Law.
- (c) The issuance of a certificate or statement of the reasons for the refusal to cash any cheque upon request of an entitled person.
- (d) the exchange of information pertaining to clients on their debit balances in order to provide necessary data to ensure safety of credit approvals, dishonest cheques information, or any other information to be exchanged between the banks, Central Bank, or any other entities approved by the Central Bank, where this exchange of information is considered by the Central Bank necessary to protect the banks.
- (e) Disclosure by a bank, in full or in part, of statements on transactions of a client necessary to substantiate a claim of the bank in a judicial dispute between the bank and the client in respect of such transactions.

The ‘confidentiality’ of the financial information included in Articles 72 and 73 is paralysed by the above exceptions stated in Article 74. Accordingly, the Central Bank of Jordan (CBJ), as a governmental agency, has the authority to obtain bank records from any bank about any client without his or her permission. Moreover, the Central Bank is not legally obliged to give the client notice to disclose his or her banks records. Therefore, the client is not entitled to object before the disclosures are made. Additionally, the exception embodied in Article 74(d) gives the financial institutions and non-financial institutions the ability to share and exchange financial information about individuals without those individuals’ consent. One major concern in this

⁸⁵ Ibid art 74.

context is that this information may be accessed and used by unauthorised personnel for identity fraud and theft.

With regards to penalties for breaching Articles 72 and 73, Article 75 of the law makes it an offence (punishable by not less than 6 months or a fine of up to JOD 50,000 or both) for persons who act contrary to above Articles.⁸⁶

6.3.3.2 The Credit Information Law No 15 of 2010⁸⁷

The *Credit Information Law of 2010* is the first legal framework of its kind in Jordan to allow the collection, use, and disclosure of personal financial information for the purposes of granting credit. The law gives the Central Bank of Jordan the authority to issue a licence for the establishment of credit reporting companies (agency) in Jordan.⁸⁸ Regardless of the fact that there is thus far no credit reporting company (agency) registered in Jordan at the time of writing (June 2011), the law is considered to be one of the most important pieces of legislation in terms of its impact on individual privacy. Under its provisions a licensed credit reporting company can obtain personal information from the following institutions: banks, financial lending companies, any company provide financial services, and/or any company approved by the CBJ to give credit reports.⁸⁹ The law restricts the credit reporting company's activities to the following:⁹⁰

- (1) the collection, storage and treatment of credit information,

⁸⁶ Ibid art 75.

⁸⁷ *Credit Information Law No 15 of 2010 (Jordan)* [Arabic] *Official Gazette* No 5034, 1 June 2003, 3071.

⁸⁸ Ibid art 3.

⁸⁹ Ibid art 9.

⁹⁰ Ibid art 11.

- (2) the provision of a special database for credit information collected for each client,
- (3) the preparation of credit reports on the forms provided by the CBJ,
- (4) the issue of credit reports on behalf of individuals based on the credit ratings, and
- (5) any other activities concerning credit information as approved by the CBJ.

For the purpose of providing credit reports, the law has defined ‘credit information’ as: any information related to individual’s identity, credit status for a period of time (unspecified in the law) which may include current and previous credit reports, current and future loans agreements, terms and conditions of these loans, repayments agreements, and their due dates.⁹¹

The law permits credit reporting companies to issue credit reports using any types of electronic means, via public or private communications networks.⁹² This means that individuals can receive, for example, their credit ratings as a text message via their mobile phones. One privacy concern may arise in such situation is that credit ratings will be treated and stored by a third party, which in this case is the telecommunications carrier. A telecommunications carrier under the current legislation may use credit information for its own benefits without obtaining individual consent.

With regards to the protection of credit information, Article 23 of the *Credit Information Law of 2010* makes it a punishable offence (up to 6 months

⁹¹ Ibid art 2.

⁹² Ibid art 16.

imprisonment and a fine of up to JOD 10,000) to disclose credit information by any person without a legitimate reason. Persons — including credit reporting company staff, credit providers and credit information providers — are required to treat credit information in a confidential manner.⁹³

Commenting on the *Credit Information Law of 2010*, the author believes that the Credit Information Law has a number of shortcomings with respect to the issue of protecting individual privacy. First, the law failed to specify the period of time for which individual credit information is to be included or excluded in the credit reports. Hypothetically, a credit reporting company can collect information about individuals since their birth. Second, the law failed to grant individuals the right to control the information being exchanged about them by the credit reporting companies. Article 18(b) only gives the Chairman of the CBJ the authority to approve the exchange of credit information between companies.⁹⁴ The Article does not require informing the individual concerned of such an exchange. It may become too difficult for an individual to know what type of information has been exchanged between these companies until the individual receives his/her credit report or rating. Further, the information may be exchanged and have adverse impacts before the individual is aware that the information has been exchanged and that the exchange has involved incorrect information. It may not only be too late for individual to correct inaccurate information in this instance, it may also be that the information may not be able to be corrected

⁹³ Ibid art 23.

⁹⁴ Ibid art 18(b).

as the individual may be unaware and unable ascertain the initiator or source of the incorrect information.

Finally, the law grants the CBJ the authority to issue regulations and/or instructions to prevent specific information to be listed in the credit reports.⁹⁵ As of 30 June 2011, no such regulations and/or instructions have been issued. Unless there are specific instructions to determine what information is to be collected, credit reporting companies are allowed to collect, store and treat any type of information that they may deem useful for them to collect in order to forward information to clients on the basis of which the client grants or declines credit applications by the individuals concerned. For example, insurance companies may request a person's information from credit reporting companies' concerning his/her medical records, and/or driving history records for the purposes of issuing insurance policies.

6.3.3.3 The Anti-Money Laundering Laws and Regulations

In reaction to the attacks of 11 September 2001 on the United States of America, the Government of Jordan has legislated a set of laws and regulations to combat money laundering and to curtail financing of terrorism activities. From 2006 to 2007, a law and relevant regulations were enacted in order to deal with these issues. The Central Bank *Circular on Regulations of Anti-Money Laundering* was introduced in 2006, and the *Anti-Money Laundering Law* was passed in 2007. It is believed that the main

⁹⁵ Ibid art 25.

reason behind these legal frameworks is the political and economical pressure imposed by the US on Jordan shortly after the September 2001 terrorist attacks.

In this section, the anti-money laundering law and regulations are carefully examined in order to determine the impacts of such regulations on personal privacy.

6.3.3.3.1 The Anti-Money Laundering Law No 46 of 2007⁹⁶

The *Anti-Money Laundering Law of 2007* was passed to strengthen the above regulations in combating criminal activities that may occur in the financial sector. The law provides a comprehensive mechanism to be implemented by all financial institutions in order to combat money laundering in Jordan. For this, Article 7 of the law creates an independent unit, called ‘The Anti-Money Laundering Unit’ (AMLU), attached to the Central Bank of Jordan (CBJ), and which is responsible, among other things, for receiving and analysing suspicious activities, requesting related information, and providing the relevant authorities with information for further actions.⁹⁷ The AMLU is also charged with the duty of preparing a report to be submitted to the Prosecutor General once there is sufficient supporting information to suspect money laundering in a suspicious transaction.⁹⁸

The *Anti-Money Laundering Law of 2007* is applicable to all banks operating in Jordan, as well as the branches of the Jordanian banks operating in a

⁹⁶ *Anti-Money Laundering Law No 46 of 2007 (Jordan) [Arabic] Official Gazette No 4831*, 17 June 2007, 4130.

⁹⁷ *Ibid* art 7.

⁹⁸ *Ibid* art 8.

foreign country. It also applies to companies involved in foreign exchange and money transfer, or companies involved in providing securities, insurance, or any other companies that are licensed to provide financial services or products (such as credit, payment and collection services, trading in money, purchasing and selling debts, financial leasing, managing investments funds), and real estate agencies.⁹⁹

The law prohibits, at the time of reporting a suspicious transaction, the disclosure — either directly or indirectly — of any information about the transaction to the customer, the beneficiary, or any other party who does not is not mandated by this law to receive such information.¹⁰⁰ However, the AMLU has the right to request any additional information from any financial institutions which may be necessary for the AMLU to perform its duties. Therefore, the relevant party is obliged to provide the requested information within the specified time period.¹⁰¹ The AMLU also has the right to request additional information from other authorities, such as judicial authorities, or any other administrative and security authorities.¹⁰² Furthermore, the AMLU has the authority to sign memoranda of understanding with its foreign counterparts to combat international of money laundering activities. Consequently, the AMLU on a reciprocal basis may provide additional information if requested by a foreign organisation.¹⁰³

⁹⁹ Ibid art 13.

¹⁰⁰ Ibid art 15.

¹⁰¹ Ibid art 17.

¹⁰² Ibid art 18.

¹⁰³ Ibid art 19.

6.3.3.3.2 Regulations of Anti-Money Laundering and Terrorism Financing Circular No 29 of 2006¹⁰⁴

In accordance with Article 99(b) of the *Banking Law*,¹⁰⁵ the Central Bank of Jordan (CBJ) has issued instructions to be implemented by all banks in Jordan in order to combat money laundering, drug-related transactions, terrorism financing risks, and other illegal activities. The regulations require banks in Jordan to conduct the Customer Due Diligence investigations (as specified in the relevant regulations) before providing certain services to the customer.¹⁰⁶ For the purpose of identification, the bank must report customer's full name, nationality, permanent residential address, phone number, work address, activity type, purpose of conducting business relationship, the names of person who are authorised to sign on the customer's behalf and their nationalities, and any other information the bank may consider necessary. With regard to minors, the bank must obtain information about the individuals who represent the minors in order for these individuals to act on behalf of the minors. The individuals who act on behalf other customers as proxies must produce a certified copy of a special power of attorney to the bank.¹⁰⁷

¹⁰⁴ *Regulations of Anti-Money Laundering and Terrorism Financing Circular No 29 of 2006, (Jordan)* <[www.http://www.cbj.gov.jo/uploads/AML.pdf](http://www.cbj.gov.jo/uploads/AML.pdf)>.

¹⁰⁵ Art 99(b) of the *Banking Law* provides that: 'The Central Bank shall issue the orders, which it deems necessary to implement the provisions of this law to be individually or collectively applicable.'

¹⁰⁶ Art 3 of the *Regulations No 29 of 2006*, defined Customer Due Diligence as: 'the identification and verification of the customer's identification and the beneficial owner and the continuous follow up on transactions that are conducted through an ongoing relationship, additionally the verification of the nature of all future relationships between the bank and the customer and its purpose.'

¹⁰⁷ *Regulations of Anti-Money Laundering and Terrorism Financing Circular No 29 of 2006 (Jordan)* art 3, s 4(a), 4(b) and 4(c).

The instructions require that the banks apply the due diligence rule in circumstances such as: (1) if a transaction is more than JOD 10,000, or the equivalent amount in other currencies, (2) if the transactions are suspected to be money laundering or terrorist financing, (3) if the transaction occurred through electronic fund transfer, regardless of the amount,¹⁰⁸ (4) if transactions were originally generated from countries that do not have adequate anti-money laundering and combating terrorism financing systems, (5) in cross-border transactions, (6) in electronic banking transactions (ATM, Internet, telephone banking), (7) in unusual transactions (cash transactions above JOD 20,000 or equivalent in other currencies, or has no economic purposes), (8) if opening accounts for non-residents, or requesting deposit boxes, cash or travel cheques.¹⁰⁹

The instructions also require that banks should maintain record-keeping facilities. For example, the banks must keep records and documents for at least five years from the time of completion of a transaction or the termination of a business relationship whichever is later. The banks are also required to maintain records and supporting evidence of transactions for at least five years in order to be used in courts if requested by any relevant authority.¹¹⁰

¹⁰⁸ Ibid art 3, s 4(a), 4(b) and 4(c).

¹⁰⁹ Ibid art 4.

¹¹⁰ Ibid art 6.

In accordance with the instructions, the employees of the bank must report to the Money Laundering Reporting Officer (MLRO)¹¹¹ any transactions are related or it could be related to illegal activities. In his/her turn, the MLRO must immediately fill out the Suspicious Activity Report (SAR) and send it to the Anti-Money Laundering Unit (AMLU) at the Central Bank of Jordan. However, the banks must not inform their clients directly or indirectly, that is, those who have inform them that these transactions have been reported to the AMLU.¹¹²

The anti-money laundering laws and regulations are required to provide some sort of stability and integrity to the financial sector in Jordan, and serve to attract legitimate foreign investments to support Jordan's economy. The author, however, believes that the anti-money laundering laws and/ or regulations in Jordan have failed to make an adequate reference to the importance of the privacy of financial personal information. This failure is due to a number of reasons.

Firstly, the anti-money laundering laws and regulations were introduced in Jordan as a result of external pressure on Jordan. The adoption of these laws was never to address an urgent and a current problem of money laundering in Jordan.

¹¹¹ The MLRO is a senior management officer who is fundamentally appointed for the purpose of reporting to the unit about suspicious transactions.

¹¹² *Regulations of Anti-Money Laundering and Terrorism Financing Circular No 29 of 2006 (Jordan)* art 7.

Secondly, it is believed that there is no limitation on the disclosure financial information (for example, personal bank accounts) permitted under the anti-money laundering laws in Jordan. The only privacy protection provisions to personal financial information are those found in the *Banking Law of 2002* concerning 'banking confidentiality'. The absence of privacy laws concerning financial information leads to the conclusion that the banking confidentiality provisions are the exceptions and the disclosure requirements within the anti-money laundering laws are the general rule.

Finally, the disclosure of personal financial information in accordance with the anti-money laundering laws is permitted when there is a suspicious activity on individual account. The laws and/or regulations grant financial institutions the discretion to decide whether or not an individual activity is suspicious. For example, transferring an amount of JOD 10,000, on a regular basis, will be still categorised as a 'suspicious' activity even though the origins of the money are identified the first time as legitimate.

The author believes that there are a number of concerns regarding the disclosure of personal financial information in the context of the anti-money laundering law. First, more personal information than ever before from many sources than ever before. Individuals will have limited opportunities to transact anonymously. Second, anti-money laundering laws and their associated regulations in Jordan do not provide a clear definition of the term 'suspicious'. It mainly relies on whether individuals are not believed to be who they say they are. Individuals will find themselves being asked to prove

their identification, and therefore, to prove their innocence. Finally, many individuals do not want their personal financial information to be made available to the public. In addition, there are some concerns that centralising collections of this type of personal information put too much power in the hands of government.

6.4 Concluding Remarks

The current chapter has examined Jordanian legal system concerning individual privacy protection. It investigated constitutional rules and laws that may be applicable to the issue of privacy. Despite the fact that the Jordanian legal system is well-structured — in terms of the constitutional separation of the three authorities (executive, judicial and legislative) — the same legal system has neglected the issue of individual privacy.

On the level of the Jordanian Constitution, the individual's right to privacy is not explicitly recognised. The protection provided within the Constitution is a basic protection to individuals in two specific situations: namely the individual's privacy at home and the privacy of an individual's communication. Constitutional protection to the right of privacy should move beyond these two situations to include the right for individual to control information concerning them.

The laws concerning individual privacy in Jordan are marred by a number of shortcomings. First, most of the major laws discussed in this chapter have neglected the right to privacy; the right to privacy is not included in the existing legislation. This is due to the fact that most of these laws were

enacted long before the new technologies emerged to play a central role in bringing the issue of privacy into the spotlight. Second, the laws concerning telecommunication and banking sectors were enacted as result of Jordan's commitment to multilateral and bilateral trade agreements. The intention of the telecommunication and banking laws is to facilitate the free flow of information rather than to restrict the flow of information by enacting privacy laws.

Third, the Jordanian legal system lacks of laws and regulations to address privacy issues arising from the new technologies. Children's online privacy, and issues related to surveillance and smart card technologies are yet to be regulated. There is an urgent need to protect individual privacy in this context, particularly the privacy of children.

Finally, Jordan's legal system has avoided implementing a comprehensive privacy protection law believing that self-regulation is a better approach. This position has been influenced by the US approach to privacy protection. The US influence is quite apparent in the strong political and economic relationship with the US. Jordan adopts similar laws and regulations to those in the US in relation to a number of issues. For example, the latest law enacted by Jordan is the *Credit Information Law of 2010* which is identical to the US law, the *Fair Credit Reporting Act*.

The author believes that Jordan is unnecessarily limiting itself by referring only to the US model and stands to benefit greatly from examining the approaches adopted by other similarly advanced jurisdictions in relation to

information privacy and other matters. This includes the European Union model that to be discussed in Chapter Eight.

A timely response to the challenges that have accompanied the adoption of new ICTs is necessary to avoid some of the worst consequences that might otherwise occur, but such timeliness should not lead to the implementation of legislation or amendment of existing legislation to allow it to better meet the current and projected needs of Jordan without adequate consideration of possible alternatives and approaches that would satisfactorily balance both the needs of the market (and relevant international demands for transparency and so forth) and the need for personal privacy protection.

Chapter Seven

The Legal Landscape of Privacy Protection in the United States

7.1 Introduction

One of the most notable features of the United States (US) legal system is that it has no comprehensive privacy law, or national authority with primary responsibility for protecting the privacy of personal information.¹ This may be justified on the ground that such legislation may undermine economic efficiency and thus adversely impact the overall economy.² This is due to the approach to privacy protection in the United States being driven by business interests, rather than embodying a rights-based approach.³ In addition, the *US Constitution* does not expressly recognise the right to privacy. For example, the US courts in their application of the *US Constitution* have held that an 'individual's expectation of privacy for information held by any third party is not legitimate, warranted or enforceable under the *Constitution*'.⁴

Furthermore, the public in the United States believe that the role of government in regulating privacy remains largely restricted to the public sector rather than the private sector. This can be seen, for example, in the *Privacy Act of 1974* (as discussed in detail further below), which was a

¹ Law Reform Commission of New Zealand, 'Invasion of Privacy: Penalties and Remedies-Review of the Law of Privacy' (Issues Paper No 14, NZLRC, 2009) 80.

² Herman T Tavani, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology* (2nd ed, 2007)161.

³ Chuan Sun, 'The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective' (2003) 2(1) *Northwestern Journal of Technology and Intellectual Property* 99, 106.

⁴ *United States v Miller*, 425 US 436 (1976).

pioneering piece of privacy legislation, but it applies only to the federal government agencies.

This chapter examines the extent to which the right to privacy is protected and maintained in accordance with the *US Constitution*. It also investigates the US privacy legislation applicable to the public sector and to the telecommunications and banking industries in the private sector.

The current chapter also provides an overview of the reasons behind the US refusal to introduce a comprehensive regulatory approach to privacy protection, and its preference for the adoption and maintenance of the self-regulatory approach. The important issue to be discussed in this chapter is the validity of the self-regulatory approach to privacy protection and whether its application is suitable for other jurisdictions, including Jordan. The chapter begins first by examining the question of a US constitutional 'right to privacy'.

7.2 Privacy as a Constitutional Right

This section examines the right to privacy in the US, as it is recognised by the *US Constitution*. This examination is crucial because the *Constitution* compels the government to use its power to act on behalf of its citizens and to create and enforce laws regulating the practices of, and transactions conducted by, citizens.⁵ In the context of privacy, the *US Constitution*⁶

⁵ Fred H Cate, *Privacy in the Information Age* (1997) 51.

⁶ *Constitution of the United States of America*, National Archives of the Government of the United States of America, <http://www.archives.gov/exhibits/charters/constitution_transcript.html> at 10 January 2009.

recognises the right to privacy in a number of its provisions and provides protection for this right in a number of ways despite the fact that the term ‘privacy’ does not exist anywhere in the *Constitution*.⁷ Despite the fact that the right to privacy is not expressly mentioned in the *US Constitution*, the US Supreme Court has ruled in favour of various privacy interests, deriving the right to privacy from the *First*, *Fourth*, and *Ninth* Amendments.⁸ The following sections present an overview of the US approach dealing with the right to privacy.

7.2.1 The First Amendment

The *First Amendment*⁹ protects three forms of privacy: (1) individuals’ ‘associational privacy’, (2) ‘political privacy’, and (3) the ‘right to anonymity in public expression’.¹⁰ Yet the concern for privacy as a right contained within the *First Amendment* was relatively late appearing. The *First Amendment* with its proclamation of the freedom of the press and religion as well as expression is couched in terms that clarify the role of government in relation to these rights: ‘Congress shall make no law ... abridging the freedom of speech, or of the press...’ having been ratified on 15 December 1791. Such a right has been cited as overriding the desire for privacy expressed by many in the public eye, thus lowering their protection from

⁷ Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (2004) 62.

⁸ Joshua B Sessler, ‘Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet’ (1996) 5 *Journal of Law and Policy* 627, 651.

⁹ The *First Amendment* provides:

‘Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.’

¹⁰ Priscilla M Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (1995) 35.

intrusion by the press and other commentators. Conversely, this same Amendment has been used to justify an expansion of privacy rights. Yet at its root is often the same cause — a desire for unfettered discussion and debate, or the free flow of information. For example, the ‘private life’ of a politician or influential actor or other public figure¹¹ is considered open to discussion and freer publication than that of an essentially private person due to their possibly greater influence on public life and decision-making, while a source of political commentary may secure the protection of anonymity under the *First Amendment* to ensure an uncensored and vigorous conduct of that same debate. There is no doubt, however, that the two ‘rights’ — the right to freedom of expression and the right to privacy — may be in conflict in a given situation; and it is here that the Court is called upon to clarify the extent of the respective rights and their applicability in given situations, as again it must in regard to the privacy right seen as inherent in the right to freedom of expression (see further below) establish its scope and limitations.

Regarding individuals’ associational and political privacy rights generally, the Supreme Court, relying on the *First Amendment*, prevents the State (both federal and state) from collecting information that would unconstitutionally compel a disclosure of group affiliation.¹² In *NAACP v Alabama*,¹³ the Court recognised that disclosure of membership information, such as names and addresses, could have highly negative consequences for the parties involved.

¹¹ *New York Times v Sullivan*, 376 US 254 (1964).

¹² Paul M Schwartz, ‘Privacy and Participation: Personal Information and Public Sector Regulation in the United States’ (1994) 80 *Iowa Law Review* 553, 567.

¹³ See *NAACP v Alabama*, 357 US 449, 462 (1958).

The Court found that ‘group privacy’ is important as a condition for individual participation in the political process. Constitutional restrictions on the State’s collection and treatment of personal information are necessary for individuals to participate in political self-government.¹⁴

With respect to the right of public expression, the Supreme Court has also found in the *First Amendment* the rights to speak, write, or publish anonymously or pseudonymously. In *Talley v California*,¹⁵ the Court found that the right to privacy is associated with the right to freedom of expression. In the right to freedom of expression is found a right to resist compelled disclosure of one’s identity, especially in the context of volatile political communications¹⁶ and the need to preserve the ‘robustness of dissent’.¹⁷

Thus a contrary right, the right not to give expression to information, is found in the right to freedom of expression. In at least one instance, a non-Federal or State government body — in this instance a local council — was held to the terms of the *First Amendment* regarding information collection and anonymity guaranteed under ‘free speech’ when its bid to compel members of a religious organisation to register in order to be able to disseminate information to a community was stymied.¹⁸ In a number of other cases,¹⁹ the

¹⁴ Schwartz, above n 12, 569.

¹⁵ See *Talley v California*, 362 US 60 (1960).

¹⁶ James Waldo, Herbert S Lin and Lynette I Millett (eds), *Engaging Privacy and Information Technology in a Digital Age* (2007)125.

¹⁷ Solove, *The Digital Person*, above n 7, 176–7.

¹⁸ For example, in *Watchtower Bible and Tract Society v Village of Stratton* 122 S Ct 2080 (2002), the right of the witnessing person to proselytise anonymously (by not being required by a Stratton Village town ordinance to be licensed prior to such an activity and supply his or her name) was upheld on the grounds of the *First Amendment*. See Solove, *The Digital Person*, above n 7, 63.

¹⁹ See *McIntyre v Ohio Election Comm'n*, 514 US 334 (1995).

Court reaffirmed its commitment to protect the right to privacy in the political context, while insisting that the government still has legitimate reasons to regulate political communications without violating this right.²⁰

However, informational privacy protection under the *First Amendment* as tested in the courts only clearly applies when government plays a role in compelling the collection of personal information²¹ and where it has a role in the treatment and dissemination of personal information collected.²² Any failure to ‘adequately account for privacy in their public record laws may be found to violate the constitutional right to privacy’;²³ and their responsibility in regard to information dissemination also comes in for scrutiny.²⁴ Government at every level and in every agency is also held to have a ‘responsibility to keep the data it collects secure and confidential absent any overriding consideration’.²⁵ One consideration which remains outstanding is that once such information enters the public domain, such protection appears to evaporate (see further below).

Personal information gathered by private actors and under no condition of governmental compulsion, however, appears not to be similarly protected by the *First Amendment*.²⁶ Here debate appears to be conducted in terms of

²⁰ Waldo, Lin and Miller, above n 16, 125.

²¹ Solove, *The Digital Person*, above n 7, 63–4.

²² Daniel J Solove, ‘The New Vulnerability: Data Security and Personal Information’ in Anupam Chander, Lauren Gelman and Margaret Jane Radin (eds), *Securing Privacy in the Internet Age*, 111, 129–30.

²³ *Ibid* 130;

²⁴ *Ibid* 130 n 108 where the author cites *Kallstrom v City of Columbus*, 136 F 3d 1055 (6th Cir 1998).

²⁵ *Ibid*.

²⁶ Solove, *The Digital Person*, above n 7, 63–4. See also 63 n 28, where the author cites Julie E Cohen, ‘The Right to Read Anonymously: A Closer Look at “Copyright Monopolies” in Cyberspace’ (1996)

whether the information itself qualifies for protection if it is of ‘personal’ rather than ‘public’ concern. For example, in *Dun & Bradstreet Inc v Greenmoss Builders Inc*,²⁷ the US Supreme Court held that personal information — here ‘speech on matters of purely private concern as opposed to speech on matters of public concern’ — cannot be protected under the *First Amendment*,²⁸ unlike material of public concern (such as material necessary for free political debate or free flow of information for commerce).

The author believes that the above Amendment does not provide sufficient protection to the right to privacy because it only applies to activities undertaken by the State (federal and state) and its agencies where such information collection is compelled by government authority. It has no application with regard to activities and practices by the private sector. Therefore, to the problem of protecting personal information from being collected and disseminated by private companies and organisations, the above Amendment does not provide any solution.

²⁸ *Connecticut Law Review* 981, 1020. Cohen argues that a federal law which punished those who tampered with photocopiers so that they could preserve their anonymity breached this provision.

²⁷ See *Dun & Bradstreet Inc v Greenmoss Builders Inc*, 472 US 749 (1985). The case summary as follows: ‘Petitioner, who was in the business of composing and selling financial reports about businesses, mistakenly reported that respondent had filed for bankruptcy. The report was sent to several of petitioner’s subscribers. Petitioner issued a corrective statement, but refused to divulge the names of those that received the report. Respondent brought a defamation suit and the jury awarded respondent presumed and punitive damages. However, a new trial was ordered because the court was dissatisfied with its jury instructions regarding petitioner’s knowledge of falsity or reckless disregard for the truth. The Supreme Court of Vermont reversed, holding that respondent was not required to show actual malice to recover presumed and punitive damages because petitioner was a nonmedia entity. On *certiorari* the Court affirmed, holding that respondent was not required to show actual malice to recover presumed and punitive damages because petitioner’s false and defamatory speech was not a matter of public concern. The Court decided that because respondent was a private party and because petitioner’s false and defamatory statements against respondent did not involve matters of public concern, respondent was not required to show petitioner acted with actual malice when making the defamatory statements to recover presumed and punitive damages.’

²⁸ *Ibid.*

7.2.2 The Fourth Amendment

The *Fourth Amendment*²⁹ of the *US Constitution* protects individuals from ‘unreasonable searches and seizures’. It requires that government officials first obtain judicial authorisation before conducting a search.³⁰ Officers must execute a traditional search warrant with dispatch, not over a prolonged period of time. If they do not find what they were looking for in a home or office listed on the warrant, for example, they must leave promptly and obtain a separate order if they wish to return to search again.³¹ Failure to meet these requirements will render their search unconstitutional and any evidence thus gathered invalid and inadmissible by court.

The most important *Fourth Amendment* cases involving privacy interests have been those dealing with wiretapping, and whether or not a ‘wiretapping’ falls under the category of ‘searches and seizure’. In *Olmstead v United States*, the majority of the Court did not apply this Amendment to wiretapping because no physical invasion had occurred. The Court in this 1928 decision rejected the attempt to make an analogy between phone conversations and mail. According to the Court, the mail is presumed confidential by the government. By contrast, ‘[t]he United States takes no such care of telegraph or telephone messages as of mailed sealed letters. There was no

²⁹ The *Fourth Amendment* states:

‘The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated; and no warrant shall issue but upon probable cause, supported by or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.’

³⁰ Solove, *The Digital Person*, above n 7, 63.

³¹ James X Dempsey, ‘Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy’ (1997) 8 *Albany Law Journal of Science and Technology* 65, 70.

searching, and there was no seizure. The evidence was secured by the use of the sense of hearing, and that only.’³²

The Court adopted the notion that the concept of privacy was based largely on a property interest. People had privacy in their ‘persons, houses, papers, and effects’.³³ However, one of the most important impacts of this case arose from Justice Louis Brandeis’ dissenting opinion, which thrust the constitutional issue of privacy into the spotlight in the United States. He made the following argument:³⁴

The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretappings. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions... Can it be that the Constitution affords no protection against such invasions of individual security?

Justice Brandeis insisted that courts must take changing conditions into account.³⁵

Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.

The above argument would prove to be prophetic as newer technologies would become available to both government and private eavesdroppers, and

³² See *Olmstead v US*, 277 US 438, 472 (1928).

³³ Regan, *Legislating Privacy*, above n 10, 37.

³⁴ See *Olmstead v US* 277 US, 438, 474 (1928).

³⁵ See *Olmstead v US* 277 US, 438, 474 (1928).

the means of communication would come to include the telephone, the fax, and electronic mail.³⁶

However, the above interpretation of the *Fourth Amendment* by the US Supreme Court has been overruled by its decision in the case of *Katz v United States* in 1967. The Court applied the *Fourth Amendment* to situations in which a person has a ‘reasonable expectation of privacy’.³⁷ This means that the Amendment:

protects people, not places, what a person knowingly exposes to the public, even in his own home or office, is not a subject of *Fourth Amendment* protection... but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.³⁸

For instance, privacy rights within this interpretation extend to a telephone booth,³⁹ and police must obtain a warrant when a search takes place in a telephone booth on a public street.⁴⁰ For the application of the *Fourth Amendment* protections, the Court used the ‘reasonable expectation of privacy’ test in order to determine the person’s right to privacy. Accordingly, there are two standards to apply this test, first: a person must ‘have exhibited an actual (subjective) expectation of privacy’ and, second, ‘the expectation must be one that society is prepared to recognise as reasonable’.⁴¹

³⁶ Harry Henderson, *Privacy in the Information Age* (1999) 63.

³⁷ See *Katz v United States*, 389 US 347 (1967).

³⁸ See *Katz v United States*, 389 US 347 (1967).

³⁹ Waldo, Lin and Miller, above n 16, 123.

⁴⁰ Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (3rd ed, 2009) 34.

⁴¹ *Ibid.*

The above approach — reasonable expectation of privacy — of the *Fourth Amendment* has two problems concerning privacy protection. First, the US Supreme Court does not apply the test of ‘reasonable privacy expectation’ to activities that take place in the public arena or to practices controlled by a third party. The *Fourth Amendment* provides no protection to individual privacy if a government agency can see his/her activity either with the naked eye, or by using advanced technology.⁴² Furthermore, the *Fourth Amendment* is inapplicable to information controlled by private sector institutions. For example, the US Court found that information about individuals held by accountants or banks has no protection under the *Fourth Amendment*.⁴³

Second, in the context of privacy information protection, the *Fourth Amendment* ignores the ability of new technology to minimise an individual’s expectation of privacy. As a result of advanced technologies, the US Supreme Court found that ‘electronic surveillance by third parties wearing a hidden audio is not subject to the Fourth Amendment’s protection’.⁴⁴ In *United States v White*, the Court stated that ‘we all know, after all, that anyone we talk with might wear such a device; thus, there can be no reasonable expectation of privacy in such conversations.’⁴⁵

The author believes that the ‘reasonable expectation of privacy’ test used by the US courts in its application to the *Fourth Amendment* is unsuited to the

⁴² Schwartz, above n 12, 572.

⁴³ See *United States v Miller*, 425 US 436 (1976).

⁴⁴ Schwartz, above n 12, 573.

⁴⁵ See *United States v White*, 401 US 745, 752 (1971).

protection of individual privacy, particularly in the context of advanced informational technologies, such as the internet, mobile phone/internet interactivity (and their vulnerability to ‘hacking’), database growth, the ease of electronic communication (email and phone) traceability and tracking, and so forth). For example, a person may have a ‘reasonable expectation of privacy’ while using the internet, but his/her personal identifiable information that is collected via such means and used by either a government agency or a third party may not be afforded protection by this Amendment, as an individual ‘expectation of privacy’ no longer exists more generally in an internet context. The understanding too that once information is on the public record (however ill-considered or even accidental that disclosure may be) that its re-publication and broad dissemination is permitted is particularly problematic, given that it has, in the past in the US, allowed the names of rape victims and juvenile offenders to be published.⁴⁶ The broad ‘third-party’ freedom to disclose information once it is in the public domain has ramifications in relation to informational privacy.

7.2.3 The Ninth Amendment

The US Supreme Court has also found constitutional protection to privacy embedded in the *Ninth Amendment* of the *US Constitution*.⁴⁷ In a landmark case, *Griswold v Connecticut*,⁴⁸ the Court located this right within the ‘penumbras’ or ‘zones’ of freedom created by an expansive interpretation of

⁴⁶ Solove, *The Digital Person*, above n 7, 67.

⁴⁷ The *Ninth Amendment* provides:

‘The enumeration in the Constitution of certain rights shall not be constructed to deny or disparage others retained by the people.’

⁴⁸ See *Griswold v Connecticut*, 381 US 479 (1965).

the *Bill of Rights*. Subsequently, the Court has handed down a line of decisions protecting certain fundamental life choices, such as abortion and aspects of one's intimate sexual life as essentially 'private', with such rights being enforceable.⁴⁹ In this case, the Supreme Court held unconstitutional a Connecticut law banning the use even by married couples of contraceptives, stating that the ban violated basic privacy precepts since it invaded 'a zone of privacy created by several fundamental constitutional guarantees'.⁵⁰ The majority of the Court supported the notion of an independent right to privacy inherent in the marriage relationship, which right was extracted from the *Ninth Amendment*.⁵¹ The Court insisted that something as intimate as the marriage relationship must stand at the centre of the zone of privacy. The decision to use contraception (and thus the right to obtain information and devices) is thus protected by the *Constitution*.⁵²

In summary, based on the above constitutional rights to privacy, the US Supreme Court has crafted a limited framework for protecting individuals' right to privacy in the context of government activities concerning personal information and no support at all for privacy rights, particularly informational privacy rights, outside the public sector.⁵³ The US constitutional protection for privacy rights protects individuals only against

⁴⁹ Solove and Schwartz, above n 40, 34. See also *Roe v Wade*, 410 US 113 (1973) which also cited the *Fourteenth Amendment*.

⁵⁰ Waldo, Lin and Miller, above n 16, 128.

⁵¹ Regan, *Legislating Privacy*, above n 10, 39.

⁵² Henderson, above n 36, 65.

⁵³ Cate, above n 5, 66. See also Solove, above n 7, 64.

government practices.⁵⁴ Those wanting protection against the private sector are forced to look elsewhere — for example, tort law, and state and federal legislation.

In order to provide a complete assessment of the US approach to privacy protection, the next section continues to search for additional provisions in the US legal system. It begins with a discussion of privacy and the law of torts.

7.3 US Privacy Torts Law

The United States has a significant body of tort law regarding invasion of privacy. Based on the 1890 article on '*The Right to Privacy*' by Samuel Warren and Louis Brandeis,⁵⁵ William Prosser in 1960 recognised four distinct torts for the invasion of privacy, which have been included in the *Restatement of the Law of Torts*.⁵⁶ These torts are: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light, and (4) appropriation.

7.3.1 Intrusion upon Seclusion

Liability for invasion of privacy exists where a person: '(1) intentionally intrudes, physically or otherwise on another's solitude, seclusion, or private affairs or concerns', which intrusion (2) 'would be highly offensive to a

⁵⁴ Maureen S Dorney, 'Privacy and the Internet' (1997) 19 *Hastings Communications and Entertainment Law Journal* 635, 639.

⁵⁵ Samuel D Warren and William D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

⁵⁶ William L Prosser, 'Privacy' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 107.

reasonable person'.⁵⁷ For example, the use of devices to oversee or overhear one's private affairs, or opening sealed mail, rifling through a person's wallet, is conduct that is an intrusion on a person's privacy and an invasion of privacy.⁵⁸ However, intrusion on privacy would not be applicable in regard to matters on the public record, such as observing or photographing someone in public place⁵⁹ unless the interference with seclusion is substantial, such that it would be considered highly offensive by an ordinary reasonable person. For example, it would not be an invasion of privacy to knock on someone's door or to call a person on the phone once or twice, but persistent hounding of a person could be characterised as an invasion.⁶⁰

The right to seclusion protects an individual against the unauthorised gathering of personal information that has never been voluntarily disclosed to the public.⁶¹ For example, a company may be liable for the tort of intrusion if it misuses highly sensitive information collected on corporate web sites.⁶² Although this tort could be applied to the information collection techniques of databases, most of the information collected is not 'highly offensive to a reasonable person'. Therefore, the tort of intrusion cannot provide an

⁵⁷ See American Law Institute, *Restatement (Second) of Torts* (1977) § 652B provides: 'One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs of concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would highly offensive to a reasonable person.'

⁵⁸ Law Reform Commission of New Zealand, 'Invasion of Privacy: Penalties and Remedies', above n 1, 75.

⁵⁹ Waldo, Lin and Miller, above n 16, 129.

⁶⁰ Law Reform Commission of New Zealand, 'Invasion of Privacy: Penalties and Remedies', above n 1, 76.

⁶¹ Dorney, above n 54, 640.

⁶² Michael L Rustad and Cyrus Daftary, *E-Business Legal Handbook* (2002) 458.

adequate safeguard against the gathering of personal information for databases.⁶³

7.3.2 Public Disclosure of Private Facts

The tort of public disclosure of private facts prohibits certain uses of personal information, regardless of how the information is collected.⁶⁴ It creates a cause of action when someone makes public ‘a matter concerning the private life of another’. This can extend to experiences in public spaces. For example, a newspaper was found liable under this tort in 1964 for publishing a photograph of a woman whose dress was blown up by the air jets in an area frequented by the public, exposing her up from the waist down (apart from her underwear). The publication caused her great embarrassment and distress.⁶⁵ The Court held that a person (here involuntarily caught in an immodest state) ‘should not be deemed to have forfeited his right to be protected from an indecent and vulgar intrusion on his right to privacy merely because misfortune overtakes him in a public place’.⁶⁶ Another example where a cause of action was established under this tort was the use of a woman’s photograph that had been taken without her permission and later accompanied a magazine story about her rare medical condition. Also published was the woman’s name and address (the Court held that this too

⁶³ Solove, *The Digital Person*, above n 7, 59.

⁶⁴ Dorney, above n 54, 641.

⁶⁵ See *Daily Times Democrat v Graham*, 162 So 2d 474 (Ala, 1964).

⁶⁶ *Ibid.*

was ‘unnecessary’).⁶⁷ In both examples, the ‘use of private facts’ was found to be a violation of this tort.

To be actionable under this tort, the matter must be communicated to the public at large or to so many persons that the matter must be regarded as substantially certain to become one of the public knowledge, not merely communicated to a third party. In this regard it is necessary to distinguish between ‘publication’ and ‘publicity’. Publication is ‘communication ... to a third person’, while ‘publicity’ is communication to ‘the public at large, or to as many persons that the matter must be regarded as substantially certain to become ... public knowledge’.⁶⁸ Thus taking private facts (for example, debt status with a particular creditor) and communicating them to a third person (an employer) is deemed not to be an invasion of privacy under this section,⁶⁹ whereas placing an advertisement in a newspaper stating the same facts or posting a sign in a window would constitute an invasion of privacy under this tort.⁷⁰

⁶⁷ See *Barber v Time Inc*, 159 SW 2d 291 (Mo, 1942).

⁶⁸ In this regard it is necessary to distinguish between ‘publication’ and ‘publicity’. Publication is ‘communication ...to a third person’, while ‘publicity’ is communication to ‘the public at large, or to as many persons that the matter must be regarded as substantially certain to become ... public knowledge’: American Law Institute, *Restatement (Second) of Torts* (1977) § 652D comment (a) thereto. See also Solove and Schwartz, above n 40, 106.

⁶⁹ American Law Institute, *Restatement (Second) of Torts* (1977) § 652D comment (a) thereto [example 1].

⁷⁰ *Ibid* § 652D [example 2]. A disclosure of bankruptcy, however, has been held not to be an invasion as bankruptcy filings are ‘a matter of public record’: *Hendry v Connor*, 303 Minn 317 at 319, 226 NW 2d 921 (1975) 923.

To be actionable under this tort, the publicised disclosure must meet two further conditions: (1) the disclosure must be ‘highly offensive to a reasonable person’ and, (2) ‘not of a legitimate concern to the public’.⁷¹

This tort applies only if the disclosure is ‘highly offensive to the reasonable person’.⁷² ‘Offensiveness’ is determined by ‘the customs of the time and place, to the occupation of the plaintiff and to the habits of his/her neighbours and fellow citizens’.⁷³ However, customs of current times have changed. It is more widely acceptable, nowadays, to disseminate information about individuals, and sometimes to do so without their consent.⁷⁴

Furthermore, giving publicity to private facts may not give the plaintiff a cause of action under this tort unless the plaintiff would be justified in feeling ‘seriously aggrieved’ by the publicity. For example, publicity given to matters such as sexual activities or sexual abuse may be offensive to a reasonable person, whereas giving publicity to facts that are merely unflattering, mildly embarrassing or annoying will not be considered an invasion of privacy.⁷⁵ In the example mentioned earlier, the creditor’s posting of a debtor’s name and status in his window constitutes an invasion of the debtor’s privacy, because of the private nature of the information disclosed (known previously only to

⁷¹ American Law Institute, *Restatement (Second) of Torts* (1977) § 652D provides: ‘One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that: (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.’

⁷² Sandra Byrd Petersen, ‘Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?’ (1995) 48 *Federal Communications Law Journal* 163, 176.

⁷³ See comment on Clause (a) (c): American Law Institute, *Restatement (Second) of Torts* (1977) § 652D.

⁷⁴ Petersen above n 72, 177.

⁷⁵ Law Reform Commission of New Zealand, ‘Invasion of Privacy: Penalties and Remedies’, above n 1, 76.

the creditor and the debtor), and the severe distress caused the debtor by the publicity given the information to the wider community.⁷⁶

However, these conditions pose two concerns for individual privacy. First, the information must be disseminated to a large number of people. That it is conditional upon being disseminated to a large number of people is a concern for the safeguarding of individual privacy.

7.3.3 False Light

The privacy right protected under this tort⁷⁷ is the right to be secure from publicity that places an individual in a false light. This tort prohibits an objectionable, false representation which does not meet the definition of defamation, and which must have been made to the general public.⁷⁸ The intent of this tort is to protect people against being cast in a false light in the public eye. For example, this tort would apply when one's photograph is publicly appeared in a way or a context that establishes negative images about him or her.⁷⁹

The false light tort and defamation tort (libel and slander) are similar but there are two major differences: firstly, 'false light' requires a wider communication of the information. It requires 'publicity' which must be made

⁷⁶ American Law Institute, *Restatement (Second) of Torts* (1977) § 652D [example 2]. A disclosure of bankruptcy, however, has been held not to be an invasion as bankruptcy filings are 'a matter of public record': *Hendry v Connor*, 303 Minn 317, 226 NW 2d 921 (1975) 923.

⁷⁷ See American Law Institute, *Restatement (Second) of Torts* (1977) § 652E, provides: '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 of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.'

⁷⁸ Dorney, above n 54, 641.

⁷⁹ Waldo, Lin and Miller, above n 16, 130.

to the public at large. Defamation requires ‘publication’, which means that the communication merely requires communications to another person.⁸⁰ Secondly, defamation is based on injury to reputation, while the false light tort is primarily intended to provide remedies for humiliation, embarrassment and other forms of mental distress.

In the context of ICT, this form of privacy may be implicated if the information disclosed concerning an individual is inaccurate or misleading, or if the custodian of computer data fails to take appropriate action to ensure the accuracy of data.⁸¹ For example, publishing someone’s photograph on the internet and writing an article underneath the photograph about corruption or drug dealings or gambling would constitute a false light action if such a person had no involvement with the material (or type of material) disclosed in the article.⁸²

7.3.4 Appropriation

The fourth category of US privacy torts involves liability for invasion of privacy where a person appropriates the name or likeness of someone else for his/her own benefit.⁸³ This tort aims at protecting a person’s pecuniary interest in the commercial exploitation of their identity (image, name, likeness and so forth).⁸⁴ The invasion can be carried out in a number of ways

⁸⁰ Solove and Schwartz, above n 40, 197.

⁸¹ Dorney, above n 55, 641.

⁸² See *Thompson v Close-up Inc*, 98 NYS 2d 300 (1950).

⁸³ See American Law Institute, *Restatement (Second) of Torts* (1977) § 652(C) states: ‘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’.

⁸⁴ Roger LeRoy Miller and Gaylord A Jentz, *Fundamentals of Business Law: Excorted Cases* (2nd ed, 2010) 91.

including: using a photograph of someone in an advertisement without their authorisation, or posing as or impersonating a person for gain.⁸⁵ There have been several cases where persons have sued on the use of their names or likenesses.⁸⁶ The appropriation tort, however, has been extended far beyond a person's actual name and likeness. Courts have held that actions such as the use for gain of well-known nicknames,⁸⁷ drawings depicting a person's profession with no distinctive facial characteristics,⁸⁸ the use of a look-alike model,⁸⁹ or of a fictitious persona created by individual,⁹⁰ as well as the imitation of a person's voice,⁹¹ are actions that give rise to an appropriation liability.⁹²

The key issue in appropriation is that this tort protects persons from the commercial exploitation for the benefit of others as a result of the use of their names or likeness or other characteristics (as above). Therefore, the use of someone's name or likeness for news, art, literature, history or biography does not create a cause of action under this tort. It excludes use incidental to the production of news broadcasts, newspapers (for example) of images of both private and public figures. A newspaper can even use someone's photograph to illustrate a story though the person in the photograph is not

⁸⁵ Law Reform Commission of New Zealand, 'Invasion of Privacy: Penalties and Remedies', above n 1, 77.

⁸⁶ See *Carson v Here's Johnny Portable Toilets Inc*, 698 F 2d 831 (6th Cir, 1983). Johnny Carson successfully sued a portable toilet company that used the name 'Here's Johnny Portable Toilets'.

⁸⁷ See *Hirsch v SC Johnson & Son Inc*, 280 NW 2d 129 (Wis, 1979).

⁸⁸ See *Ali v Playgirl Inc*, 447 F Supp 723 (SDNY, 1978).

⁸⁹ See *Onassis v Christian Dior*, 472 NYC 2d 254 (NY Supp, 1984).

⁹⁰ See *Productions Inc v Day & Night Co*, 523 F Supp 485 (SDNY, 1981).

⁹¹ See *Midler v Ford Motor Co*, 849 F 2d 460 (9th Cir, 1988).

⁹² Solove and Schwartz, above n 40, 210-11.

the actual person in the story as the use is not an appropriation because it was not being used for commercial benefits (such as product endorsement).⁹³

This tort is been applied ‘almost exclusively’⁹⁴ to the use of public figures’ names and likeness to sell products or services for commercial benefits without the public figures’ consent. Thus this tort recognises for public figures a property right to their names and likenesses which can be protected, but given what appears to be a lack successful cases exploring the rights of private persons to protect their image, name and other identifying details from commercial exploitation, it appears that the right to privacy in instances where the personal information of ordinary individuals is used by third parties for commercial profits may remain beyond the scope of the tort of appropriation.⁹⁵

Unfortunately, the adoption of the right to property in the tort of appropriation has not provided an effective tool to address privacy concerns and particularly in the context of telemarketing technologies. This is because such tort aims at protecting someone’s economic benefits in a form of property, and it is most effective at protecting public figures that have created value in their ‘personalities’. These are not the same benefits involved with a right to privacy, which can be implicated regardless of the economic value and interest accorded to one’s name or likeness.⁹⁶

⁹³ See *Arrington v New York Times*, 434 NE 2d (NY Ct App, 1982).

⁹⁴ Petersen above n 72, 177.

⁹⁵ Petersen above n 72, 177.

⁹⁶ Solove, *The Digital Person*, above n 7, 61.

7.4 US Federal Legislations Applicable to Privacy

It has stated above that the United States has no comprehensive privacy law governing the collection, use, and distribution of personal information by the public or private sector. Instead, the US Congress has passed a variety of laws and regulations, each of which addresses privacy information practices (for example, the collection, use, disclosure, dissemination, and so forth) in particular sectors. This section examines US laws for the protection of the privacy of personal information in three main sectors: the public sector, the telecommunications sector, and the financial services sector. For the public sector, a number of US laws shall be investigated. These laws include: the *Privacy Act of 1974*, the *Freedom of Information Act (FOIA) of 1966*, *Electronic of Freedom of Information Act of 1986*, the *Computer Matching and Privacy Protection Act of 1988*, and the *e-Government Act of 2002*.

With regards to US laws in the telecommunications sector, the following are included in the discussion: the *Electronic Communications Privacy Act of 1986*, the *Telephone Consumer Protection Act of 1991*, and the *Children's Online Privacy Protection Act of 1998*.

With respect to the US privacy laws in the financial sector, a number of laws are subject to discussion including: the *Gramm-Leach-Bliley Act of 1999*, the *Fair Credit Reporting Act*, the *Right to Financial Privacy Act of 1978*, and the *Bank Secrecy Act of 1970*.

7.4.1 Privacy Laws Concerning the Public Sector

Despite the fact that the US Federal Government is the world's largest collector and user of personal information,⁹⁷ controls on its collection and dissemination practices are limited.⁹⁸ There a number of laws that provide the means for regulating the privacy information practices in the public sector. Below is a brief overview of the main laws that protect personal privacy from identified conduct by government with regard to the collection, use, transfer and disclosure of personal information.

7.4.1.1 Privacy Act of 1974

In response to concerns about the potential power of the government to use and abuse personal information about its citizens,⁹⁹ Congress enacted the *Privacy Act of 1974*.¹⁰⁰ The Act mainly provides four safeguards against an invasion of privacy: (1) 'permitting an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by agencies', (2) 'permitting an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent',¹⁰¹ (3) 'allowing an individual to access and correct his personal information', and, (4) 'ensuring

⁹⁷ Cate, above n 5, 76.

⁹⁸ Jonathan P Cody, 'Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation' (1999) 48 *Catholic University Law Review* 1183, 1197.

⁹⁹ Jacqueline Klosek, *Data Privacy in the Information Age* (2000) 134.

¹⁰⁰ See *Privacy Act of 1974* 5 USC § 552a.

¹⁰¹ See *Privacy Act of 1974* 5 USC § 552a (b).

that information about an individual is current and accurate, and allowing an individual to make amendments if needed'.¹⁰²

Although the above provisions provide considerable protection for individual privacy, the *Privacy Act* has a number of limitations. First, it only applies to federal agencies, not to businesses or private organisations. Furthermore, it does not apply to US state and local agencies.¹⁰³ Second, the law contains a number of exemptions that permit disclosure of information to other government agencies. For example, individual consent is not necessary if an agency decides to disclose information for any 'routine use' if the disclosure is 'compatible' with the uses for which the information was collected.¹⁰⁴ The 'routine use' exemption has been described as 'a huge loophole' as government agencies have used it to justify 'any use' of personal information.¹⁰⁵ For example, in order to detect fraud, the federal government investigated thousands of employees' files in 1977 to match them with records held by other government agencies. Despite this sharing of records between different agencies violating the *Privacy Act*, it was justified under the 'routine use' exception.¹⁰⁶

Although the *Privacy Act* requires an individual's consent before his or her information can be disclosed, redress for violations of the Act is virtually

¹⁰² See *Privacy Act of 1974* 5 USC § 552a (d).

¹⁰³ Solove and Schwartz, above n 40, 658.

¹⁰⁴ Catherine Louisa Glenn, 'Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records' (2000) 53 *Vanderbilt Law Review* 1605, 1625.

¹⁰⁵ Cate, above n 5, 78.

¹⁰⁶ Regan, *Legislating Privacy*, above n 10, 86.

impossible to obtain.¹⁰⁷ The *Privacy Act* provides individuals with a monetary remedy for disclosures of personal information only if the disclosure was made ‘willfully and intentionally’.¹⁰⁸ This restriction on recovery of damages fails to redress the most common form of disclosure, namely in error, due to carelessness, for example. This leaves little incentive to bring suit.¹⁰⁹ For example, in *Andrew v Veterans Administration*, Veterans Administration released inadequately redacted personnel records of nurses resulting in what the court called a ‘substantial’ violation of nurses’ privacy. However, the agency could not be sued under the *Privacy Act* because it acted negligently, not willfully.¹¹⁰ Thus, individuals who seek to enforce their rights under the *Privacy Act* face numerous statutory challenges, limited damages and scant chance to affect an agency’s overall behaviour.¹¹¹

Finally, the *Privacy Act* is not applicable when the disclosure of personal information is made under the *Freedom of Information Act* (FOIA). This means the FOIA provides an exception to the obligation to protect personal information, and personal information may be disclosed from one government agency to another or even to a private organisation without violating the *Privacy Act*. However, the two laws will be examined and compared in the following section.

¹⁰⁷ Solove, *The Digital Person*, above n 7, 136.

¹⁰⁸ *Privacy Act of 1974* 5 USC § 552a (g)(4).

¹⁰⁹ Daniel J Solove, 'Access and Aggregation: Public Records, Privacy and the Constitution' (2001) 86 *Minnesota Law Review* 1137, 1169.

¹¹⁰ *Ibid.*

¹¹¹ Schwartz, above n 12, 596.

7.4.1.2 Freedom of Information Act of 1966

The *Freedom of Information Act* (FOIA) was enacted in 1966 and twice amended, in 1974 and 1986.¹¹² While the *Privacy Act* focuses on an individual's right to obtain records pertaining to themselves, the FOIA attempts to make information concerning government activities available to the public.¹¹³ Under the FOIA 'any person' (including associations, organisations, and foreign citizens) may request records maintained by an executive agency.¹¹⁴ The FOIA extends its applications to all records held by government agencies, including any records obtained by an agency through the internet.¹¹⁵ However, the right of an individual to obtain information under the FOIA is not absolute. The FOIA contains nine enumerated exemptions to disclosure.¹¹⁶ If the information or records falls within any one of these exemptions, the government agency to whom the request has been made may withhold the information or records from public.¹¹⁷ Two of these exemptions are designed to protect individual privacy.

The first exemption is under section 552(b)(6) which states that disclosure requirements under the FOIA do not apply to:¹¹⁸

Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

¹¹² *Freedom of Information Act* 5 USC § 552.

¹¹³ Henderson, above n 36, 47.

¹¹⁴ Solove, 'Access and Aggregation', above n 110, 1161.

¹¹⁵ Cody, above n 98, 1199.

¹¹⁶ See *Freedom of Information Act* 5 USC § 552 (b).

¹¹⁷ Anthony T Kronman, 'The Privacy Exemption to the Freedom of Information Act' (1980) 9 *Journal of Legal Studies* 727, 729.

¹¹⁸ See *Freedom of Information Act* 5 USC § 552.(b)(6).

The second exemption is under section 552(b)(7)(c) which prohibits the release of:¹¹⁹

Records or information compiled for the law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy.

Although exemption under section 552(b)(6) seems to provide for a simple task of withholding records to protect individual privacy, government agencies may attempt to use this exemption to protect their own privacy.¹²⁰ For instance, a landmark case (decided by the US Supreme Court) where a government agency attempted to hide behind the privacy exemption is *Department of Air Force v Rose*.¹²¹ The facts of this case are summarised as follows:¹²²

The plaintiffs [Rose] requested copies of case summaries of Honor Code hearings at the Air Force Academy, “with personal references or other identifying information deleted.” The summaries ... contained brief reports of formal hearings at the Academy regarding alleged violations of the Honor Code (under which every cadet pledges not to lie, cheat or steal, or “tolerate” another cadet who does. Hearings of this sort are held before an Honor Board composed of cadets and may have one of three possible outcomes: the accused cadet may be found guilty, not guilty, or guilty “with discretion”. According to the Academy practice, regardless of the outcome, a report of each Honor Board hearing is posted on bulletin boards throughout the Academy and distributed to faculty and administrators. However, except where the verdict is guilty without “discretion”, the name of the cadet is deleted from the publicised case summary.

¹¹⁹ See *Freedom of Information Act* 5 USC § 552 (b) (7)(c).

¹²⁰ Kimera Maxwell and Roger Reinsch, 'The Freedom of Information Act Privacy Exemption: Who Does It Really Protect?' in Theodore R. Kupferman (ed), *Privacy and Publicity* (1990) 88.

¹²¹ See *Department of the Air Force v Rose*, 425 US 352 (1976).

¹²² Kronman, above n 117, 758-9.

The Air Force Academy refused to grant the plaintiffs' request claiming, among other things, that disclosure of the case summaries would constitute a serious invasion of the personal privacy of [the cadets concerned].

The US Supreme Court rejected the claim and concluded that Exemption 6 does not create a blanket exemption for personnel files. Regardless of whether the documents whose disclosure is sought are in 'personnel' or 'similar' files, nondisclosure is not sanctioned unless it can be demonstrated that it would be a clearly unwarranted invasion of personal privacy.¹²³ Therefore, the Court found that the files did not contain the 'vast amounts of personal data' that constitute a personnel file, nor was access to these files drastically limited, so the Exemption 6 claim was not applicable.¹²⁴

Secondly, in regard to exemption under section 552(b)(7)(c) of the FOIA, in *United States of Justice v Reporters Committee for Freedom of the Press*, the Supreme Court noted the need to balance the interests of openness and accountability against the statutory recognition of individual privacy.¹²⁵ In this case, an application was submitted by the Reporters Committee for Freedom of the Press (respondents) to obtain information regarding criminal records of four members of the Medico family (a family with a legitimate business controlled by organised crime figures). The information requested included any arrests, indictments, acquittals, convictions, and sentences of the four family members. Although the FBI originally denied the request, it provided information regarding three of the Medico family members after

¹²³ See *Department of the Air Force v Rose*, 425 US 352 (1976).

¹²⁴ Maxwell and Reinsch, above n 120, 90.

¹²⁵ Waldo, Lin and Miller, above n 16, 132.

their death. The respondents requested the criminal records of the fourth member, Charles Medico, but their request was denied in accordance with Exemption 7(c) of the FOIA.¹²⁶

The Court addressed whether disclosure of the criminal record ('rap sheet') constituted an unwarranted invasion of privacy within the meaning of Exemption 7(c) of the FOIA. The Court held that:¹²⁷

The fact that an event was not wholly "private" did not mean that an individual had no interest in limiting its disclosure. The privacy interest in a rap sheet was substantial. Whether an invasion of privacy was warranted had to turn on the nature of the requested document and its relationship to the basic purpose of the FOIA, which focused on the citizen's right to be informed about the government's actions. The news groups in this case did not intend to discover anything about the conduct of the agency, and response to the request would not shed any light on the agency's conduct. Thus, the public interest in release of a rap sheet was not the type of interest protected by the FOIA. The court held, as a categorical matter under Exemption 7 (c) that a third party's request for law enforcement records about a private citizen could reasonably be expected to invade that citizen's privacy, and that when the request sought no official information about the government, the privacy invasion was unwarranted.

The above two privacy exemptions in the FOIA merely provide grounds for agencies to refuse to disclose information if they desire. The FOIA grants discretionary grounds for release of personal information only if the public

¹²⁶ Solove and Schwartz, above n 40, 607.

¹²⁷ See *United States Department of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989).

interest in regard to a federal government or agency performance or activity outweighs the individual's privacy interest in the information.¹²⁸

The above discussion may lead to the conclusion that the relationship between the FOIA and the *Privacy Act* in the United States is somewhat complex. An application to request information in accordance with the FOIA may lead to three possible outcomes. First, in instances where the FOIA requires the release of information, the *Privacy Act* cannot prevent its release. The *Privacy Act* explicitly exempts from its nondisclosure obligations information for which the FOIA requires disclosure. However, the privacy exemptions (above) under the FOIA will limit the amount of personal information that must be released under this law. Secondly, in instances where the FOIA does not require disclosure and personal information is requested by a third party, a government agency can rely on the use of *Privacy Act* to prevent the release of such information. Thirdly, in instances where the FOIA does not require release of personal information and such information is requested by the person to whom the information requested pertains, the *Privacy Act* can require that information's release to the requester.¹²⁹ An essential concept regarding the FOIA is that it sometimes requires the government to disclose information, but never requires nondisclosure.¹³⁰

¹²⁸ Schwartz, above n 12, 593 where the author cites 5 USC 552(b)(1)-(9).

¹²⁹ Schwartz, above n 12, 593.

¹³⁰ Ibid, where the author cites *Chrysler Corp. v Brown*, 441 US 228, 292 (1979).

7.4.1.3 Electronic Freedom of Information Act Amendments of 1996

Responding to rapid ICT developments and the wide use of computer databases and information systems by federal government agencies, the US Congress passed the *Electronic Freedom of Information Act Amendments* (E-FOIA) in 1996¹³¹ to enable any person to access records stored in electronic devices (including e-mail messages) in the same way he or she could access paper records.¹³² The importance of such amendments is their recognition of the changing nature of government information. The E-FOIA is to be applied to the information itself, rather than the form of the information. It is not intended to apply to the tangible documentation, but the information contained therein.¹³³ The law requires government agencies to establish an index of the documents they possess and make the index available on the internet.¹³⁴ Furthermore, it also requires the agencies to establish 'electronic reading rooms' where people can read documents online. These rooms must contain documents that are likely to be requested multiple times.¹³⁵ However, the E-FIOA has the same exemptions in relation to disclosure requirements as those stated in the FOIA of 1966. With regard to personal privacy, the E-FOIA does not apply to 'personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy',¹³⁶ and 'records or information compiled for law

¹³¹ *Electronic Freedom of Information Act Amendments of 1996* 5 USC § 552.

¹³² *Electronic Freedom of Information Act Amendments of 1996* 5 USC § 552(a)(2).

¹³³ Robert Ratish, 'Democracy's Backlog: The Electronic Freedom of Information Act Ten Years Later' (2007) 34 *Rutgers Computer & Technology Law Journal* 211, 221–2.

¹³⁴ *Electronic Freedom of Information Act Amendments of 1996* 5 USC § 552(a)(2).

¹³⁵ *Electronic Freedom of Information Act Amendments of 1996* 5 USC § 552(a)(2).

¹³⁶ *Electronic Freedom of Information Act Amendments of 1996* 5 USC § 552(b)(6).

enforcement purposes, but only to the extent that the production of such law enforcement records or information, could reasonably be expected to constitute an unwarranted invasion of personal privacy'.¹³⁷

In the author's view, it seems that the impact of advanced technology — which allows public agencies to collect personal information and makes it easier for third parties to search, access and transfer such information — is an important factor compelling law makers in the US to enact the E-FOIA.

Both freedom of information laws (FOIA and E-FOIA) aim to ensure public access to information held by government agencies in order to make government officials more accountable for their actions and decisions, and ensure public access to information concerning public policy. This may also serve also the protection of personal information held in the public records. Government agencies and officials will be more accountable for, and transparent in regard to, the protection of personal information. Officials will be more diligent in regards to the disclosure of personal information and more careful with the treatment of such information. This, in the longer term, serves the maintenance of the right to privacy in the public sector.

7.4.1.4 Computer Matching and Privacy Protection Act of 1988

Computer matching or 'data-matching' is a variation on the technology used to merge computerised records. It involves cross-checking information in

¹³⁷ *Electronic Freedom of Information Act Amendments of 1996* 5 USC § 552(b)(7).

two or more unrelated databases to produce matching records.¹³⁸ Computer matching has been used by various government agencies for a number of purposes, such as: identifying individuals who may be of interest to the government agency conducting the match (for example, by detecting individuals who may have received excessive benefits by error, or failed to pay appropriate taxes).¹³⁹

Computer matching practices that involve personal information raise a number of privacy concerns. A major concern is that the practices can uncover large quantities of previously unknown personal information about individuals.¹⁴⁰ This concern is exacerbated by the fact that computer matching can occur without the knowledge or consent of the data subject, thereby limiting the ability of the data subject to seek access to information derived from computer matching. Another concern relates to the accuracy of the information derived from computer matching. If the information gathered is incorrect or incomplete at the time of collection, or ceases to be accurate some time after collection, the information generated by this technique will be inaccurate. Further, there is concern about the storage of large amounts of personal information gathered for the purpose of computer matching.¹⁴¹

¹³⁸ Tavani, above n 2, 141.

¹³⁹ Roger Clarke, *Dataveillance by Governments: The Technique of Computer Matching* (1993) Xamax Consultancy Pty Ltd <<http://www.rogerclarke.com/DV/MatchIntro.html>> at 27 January 2010.

¹⁴⁰ Vladimir Estivill-Castro, Ljiljana Brankovic and David L Dowe, *Privacy in Data Mining* (1999) Privacy Law and Policy Reporter <<http://www.austlii.edu.au/au/journals/PLPR/1999/44.html>> at 27 January 2010, reprint of article originally appearing (1999) 35(7) *Official Journal of the Australian Computer Society (NSW Branch)*.

¹⁴¹ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 403.

To address the above concerns, the United States Congress passed the *Computer Matching and Privacy Protection Act of 1988* (CMPPA) as an amendment to the *Privacy Act*.¹⁴² Due to the ‘routine use’ of data loophole in the *Privacy Act*, the Act provided little protection to individuals who were subject to computer matching. As a result, government agencies were able to skirt the *Privacy Act’s* requirement that individuals consent to the use of information for a purpose other than the one initially intended.¹⁴³ Therefore, the Act of 1988 prevents government agencies from disclosing records to other agencies to be used in a computer matching program, unless there is a written agreement between these agencies which specifies — among other things — the following: (1) the purpose and legal authority for conducting the program, (2) the justification for the program, and (3) a description of the records that will be matched.¹⁴⁴ In order to protect individuals’ records in computer matching programs, the Act requires that government agencies must not take any action against any individual based on information obtained by computer matching unless the agency has independently verified such information.¹⁴⁵ The Act also requires government agencies involved in computer matching programs to develop policies and procedures that must be approved by an Agency Data Integrity Board.¹⁴⁶ A Guidance document issued by the Office of Management and Budget (OMB) on interpreting the

¹⁴² *Computer Matching and Privacy Protection Act of 1988* 5 USC § 552a.

¹⁴³ Paul M Schwartz and Joel R Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996) 101.

¹⁴⁴ *Computer Matching and Privacy Protection Act of 1988* 5 USC § 552a(2).

¹⁴⁵ *Computer Matching and Privacy Protection Act of 1988* 5 USC § 552a(2).

¹⁴⁶ *Computer Matching and Privacy Protection Act of 1988* 5 USC § 552a(4).

Act states that policies and procedures for such programs may include the following:¹⁴⁷

1. Purpose and legal authority: As the CMPPA provides no independent authority for the operation of matching programs; agencies should cite a specific Federal or State statutory or regulatory basis for conducting such programs.
2. Justification and expected results: The reason/s for computer matching being conducted (as opposed to other administrative activity) and the expected results to be provided by the government agency.
3. Records description: An identification of the Federal of system(s) of records or non-Federal records involved, including the number of records, data elements included in the match.
4. Notice procedures: A description of the individual and general periodic notice procedures.
5. Verification procedures: A description of the methods that the agency will use to independently verify the information obtained through the matching program.
6. Disposition of matched items: A statement that information generated through the match will be destroyed as soon as it has served the matching program's purpose (unless retention is otherwise legally required).

¹⁴⁷ Office of Management and Budget, 'Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988', 54 Fed Reg 25818-25829, 25826 (1989) OMB
<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf> at 3 February 2011.

7. Security procedures: A description of administrative and technical safeguards to be used to protect the information. These should be commensurate with the level of sensitivity of the data.
8. Records accuracy assessment: Any information regarding accuracy of the records being matched. Note; the *Privacy Act* requires Federal agencies maintain records so as to ‘reasonably assure fairness in any determination made on the basis of the record’. The act also requires that such agencies take ‘reasonable steps to ensure the accuracy of records disclosed to non-Federal recipients’.¹⁴⁸
9. Comptroller General: A statement that such party may have accesses all records of recipient agency or non-Federal agency to monitor or verify compliance.

The above requirements may lead to the conclusion that there is no overarching independent regulatory authority in the United States to oversee the implementation of the above procedures. (Inspection by the Comptroller General is permitted not made mandatory.) An agency Data Integrity Board considers and approves proposed computer matching exercises (in terms of an existing interagency data-matching agreement)¹⁴⁹ but this in itself may not be effective in protecting the data generated from the matching programs. This lack of a strong overarching central authority is an indication that the US approach to privacy protection, particularly in this area (data-

¹⁴⁸ Ibid.

¹⁴⁹ Ibid.

matching), favours a piecemeal approach in the form of guidelines and procedures rather than a comprehensive legislative approach to privacy.

7.4.1.5 E-Government Act of 2002

The launch of the e-government website in the United States in 2000¹⁵⁰ has made it easier than ever for government agencies to obtain and process personal information about citizens and residents in many ways and for diverse purposes. However, in order to enhance the protection of individuals' personal information in the context of e-government, the US Congress passed the *E-Government Act of 2002*.¹⁵¹ The Act requires that government agencies must conduct a privacy impact assessment (PIA) in the following circumstances: (1) before the agencies develop or procure information technology to collect, maintain, or disseminate information that is in a personally identifiable form;¹⁵² or (2) before they initiate any new data collections involving personal information that will be collected, maintained, or disseminated using information technology channels.¹⁵³ This includes (among others) the conversion of paper records to electronic records; wherever anonymous records are to have anonymity removed; where the adoption of new technology makes existing information more easily accessible or public access available via a new means; where significant data merging will occur or additional data makes identification more likely; and

¹⁵⁰ The USA.gov website is an initiative administered by the US General Services Administration's Office of Citizens Services and Innovative Technologies (GSA). USA.gov went online on 22 September 2000 initially as 'FirstGov.gov'. The GSA and 22 federal agencies funded the initiative in 2001 and 2002. Since 2002, USA.gov has received an annual appropriation from the US Congress. In January 2007, FirstGov.gov officially changed its name to USA.gov.

¹⁵¹ *E-Government Act of 2002* 44 USC § 208.

¹⁵² *E-Government Act of 2002* 44 USC § 208

¹⁵³ *E-Government Act of 2002* 44 USC § 208.

where interagency data sharing is for a new purpose.¹⁵⁴ In addition, the Act requires agencies, where practicable, to make PIA results publicly available through the agencies' websites, in publication in the Federal Register, or by any other means.¹⁵⁵ According to the relevant Guidance issued by the OMB, a PIA is 'an analysis of how information is handled,' conducted so as

(i) to ensure that the treatment of personal information conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate procedures and alternative processes [adopted by the agencies] for handling information to mitigate potential privacy risks.¹⁵⁶

Consequently, the US federal agencies are required, in accordance with the *E-Government Act*, to include on their websites a privacy notice that states what information is to be collected, why it is being collected, its intended use, what notice or opportunities for consent are available to individuals regarding what is to be collected and how it will be shared, and how it will be secured.¹⁵⁷

The author's assessment of the above US laws concerning individual privacy in the public sector is that the individual's ability to enforce his/her privacy

¹⁵⁴ Office of Management and Budget, *Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (26 September 2003) <http://www.whitehouse.gov/omb/memoranda_m03-22/> at 30 December 2010. See Attachment A(II)(B)(a).

¹⁵⁵ *E-Government Act of 2002* 44 USC § 208. See also Office of Management and Budget, *Explanatory Memoranda M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, above n 144. See Attachment A. (II)(C)(c).

¹⁵⁶ Office of Management and Budget, *Explanatory Memoranda M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, above n 154.

¹⁵⁷ Janice Warner and Soon Ae Chun, 'Privacy Protection in Government Mashups' (2009) 14(1/2) *Information Polity* 75, 76.

rights is almost paralysed. The existence of different federal agencies, each of which may have a different privacy regulatory framework, may result in each one of these agencies having different compliance policies as each has the right to create its own policies and guidelines that suit its own activity.

Furthermore, it is worth mentioning that the US legislation discussed above does not govern the activities of businesses and private entities. Such activities (either between businesses or between businesses and individuals) are totally outside the scope of the above legislation; they do not cover violation of personal privacy in the private sector. For this reason, it is necessary to provide an assessment of privacy protection in the US private sector. In order to do this, an investigation in two major sectors will be undertaken: those of telecommunications and financial services. These two areas were chosen for a number of reasons: (1) both sectors are among the largest in the private sector in terms of their ability to collect, use and transfer personal information, (2) these two sectors are involved in cross-border data exchange and international data flow, which in turn, may lead to the issue of a conflict of legislation with one or more jurisdictions, and (3) US privacy laws concerning these two sectors may have a significant impact on other jurisdictions (such as Jordan). For instance, the definition of 'personal information' provided on the Jordanian Telecommunications Regulatory Commission (TRC) website is identical to the definition stipulated in the *US Children's Online Privacy Protection Act (COPPA) of 1998* (as will be examined below). The first privacy laws to be examined are those applicable to the US telecommunications sector.

7.4.2 Privacy Laws Concerning US Telecommunications Sector

Since the deregulation of telecommunications sector during the 1980s, the characteristics of the communications market and communications services have evolved significantly in the United States and around the world.¹⁵⁸ Telecommunication services have now become a significant tool for individuals, businesses and governmental agencies to perform daily activities. Individuals, businesses and government rely on telecommunications networks to send and receive messages via the Internet. Businesses are creating their own private networks to reach large number of customers. The government agencies, too, use telecommunications technologies to fulfill their public service responsibilities. In order to provide services, the telecommunications service providers have to handle large volumes of personal information that jeopardise personal privacy. In order to protect people's privacy in this context, a number of laws were enacted in the United States to deal with the protection of personal information in the context of the telecommunications sector. These laws are:

7.4.2.1 Electronic Communications Privacy Act of 1986

The *Electronic Communications Privacy Act of 1986*¹⁵⁹ (ECPA) was enacted to extend the protection of individual privacy in light of dramatic changes in computer and telecommunications technologies.¹⁶⁰ The ECPA is intended to create a balance between privacy and law enforcement by supporting the

¹⁵⁸ Schwartz and Reidenberg, above n 143, 220.

¹⁵⁹ *Electronic Communications Privacy Act of 1986* 18 USC § 2510.

¹⁶⁰ Henry M Cooper, 'The Electronic Communications Privacy Act: Does the Answer to the Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis' (2001) 20 *John Marshall Journal of Computer & Information Law* 1, 2.

development and use of these technologies and services. The law aims at encouraging the proliferation of new communications technologies, but it recognised that individuals would not trust new technologies if their privacy is not protected.¹⁶¹

The ECPA covers all types of electronic communications, including data transmissions between computers, paging and devices, electronic mail (e-mail), and video transmissions, and prohibits unauthorised eavesdropping by all persons and businesses.¹⁶² Although the ECPA protects all these types of transmissions, it does not protect against the collection of transactional data generated by these transmissions. An electronic communication service provider is even expressly permitted, without notice or subscriber consent, to disclose transactional information concerning the subscriber to any person, other than government entity, for any purpose.¹⁶³

The ECPA prohibits the interception, use or disclosure of the contents of wire, oral, and electronic communications, by private and public parties unless specifically authorised by statute or by a warrant issued on probable cause.¹⁶⁴ The prohibition includes: accessing, obtaining, altering or transferring of electronic communications by businesses or individuals.¹⁶⁵ However, there are two exceptions to this general prohibition.

¹⁶¹ Dempsey, above n 31, 74.

¹⁶² *Electronic Communications Privacy Act of 1986* 18 USC § 2510.

¹⁶³ Suzanne M Thompson, 'The Digital Explosion Comes with a Cost: The Loss of Privacy' (1999) 4 *Journal of Technology Law and Policy* 3, 40.

¹⁶⁴ Klosek, above n 99, 138.

¹⁶⁵ Dorney, above n 54, 644.

First: the Act does not apply if there is consent of one of the communicating parties.¹⁶⁶ For example, a person may secretly tape and record his/her communication with another. Therefore, it is not illegal under this Act to secretly record one's own telephone conversations,¹⁶⁷ (though it may be under State law without all party consent). It should also be noted that 'record' and 'divulge' (to a third party, for example) are two different concepts and may be viewed entirely differently in terms of legality, remedy and so forth.)¹⁶⁸

Second: a private electronic communications services provider (such as an employer) is permitted to intercept, disclose, or use any communications in the normal course of employment while engaged in an activity incident to rendering the service or to protecting the providers' rights or property.¹⁶⁹ Furthermore, system operators may intentionally disclose the contents of any stored communications to the proper authorities when criminal activities are afoot; with the consent of the originator, addressee, or intended recipient; or to any intermediary provider.¹⁷⁰

The ECPA requires law enforcement to obtain a court order by submitting an application that includes an extensive list of legal requirements before intercepting any communication covered by this law. The list of legal

¹⁶⁶ *Electronic Communications Privacy Act of 1986* 18 USC § 2511(2)(c).

¹⁶⁷ Solove and Schwartz, above n 40, 300.

¹⁶⁸ Reporters Committee for Freedom of the Press, 'Can We Tape? State-by-State Guide [to legislation]' <<http://www.rcfp.org/taping/states.html>> at 2 March 2011. Eg, Maine one party consent, Washington all party consent required for recording it should be noted that record and divulge are different concepts.

¹⁶⁹ Dorney, above n 54, 644.

¹⁷⁰ *Electronic Communications Privacy Act of 1986* 18 USC § 2511(3).

requirements include: proper authorisation from the appropriate official, and the identification of the investigators, the crimes, and the parties to be intercepted specified, a full and complete statement of the facts and circumstances relied on by the applicant to justify the belief that the order should be issued, the goals of the interception, the duration of the interception, including when it will begin and end, the actual hours of interception per day, and the days of the week of interception, exhaustion and necessity, minimisation, and the equipment and technology to be used.¹⁷¹

The reason behind the list of legal requirements is that intercepting electronic communication poses a greater threat to individual privacy than the physical searches and seizures cover by the *Fourth Amendment* (as previously discussed). Interception of electronic communication inevitably captures some communications that may not be relevant to the investigation by law enforcement bodies. Further, unlike a typical search warrant, the interception of electronic communications is carried out surreptitiously and is conducted as long as the objectives of the investigations are achieved. The investigation may continue for months and may involve thousands of intercepted communications.

The ECPA provides both criminal¹⁷² and civil remedies¹⁷³ in the event of violation. Civil suits are more common because it is unclear whether public prosecutors will be interested in disputes between operators, employers, and

¹⁷¹ *Electronic Communications Privacy Act of 1986* 18 USC § 2518.

¹⁷² *Electronic Communications Privacy Act of 1986* 18 USC § 2511(4)(a).

¹⁷³ *Electronic Communications Privacy Act of 1986* § 2520

users.¹⁷⁴ Appropriate relief for individuals and/or entities damaged as a result of a violation of the statute may include: preliminary, equitable or declaratory relief, where appropriate;¹⁷⁵ actual damages,¹⁷⁶ attorney's fees and court costs.¹⁷⁷

7.4.2.2 Telephone Consumer Protection Act of 1991

Prior to the *Telephone Consumer Protection Act of 1991* (TCPA), there was no substantial federal regulation of telephone solicitations. However, by 1990 over 30,000 businesses engaged in telemarketing and 300,000 telephone solicitors (call centre employees) were contacting more than 18 million Americans every day, resulting in sales of approximately USD 435 billion in goods and services.¹⁷⁸ It is believed that unwanted telephone calls (telephone solicitations) violate individual privacy in two ways: (1) it violates individual's right to be left alone in their homes. Most people (consumers, legislators and academics) would regard unwanted telephone calls as a nuisance that involves the most basic sort of privacy — the right to be let alone in one's home (for example, in the view of most people, receiving unwanted calls during dinner constitutes an invasion of someone's privacy).¹⁷⁹ (2) Companies (telemarketers) that use telephone solicitations may have access to a large amount of personal information about individuals' (for example, buying habits, beliefs, race, income, and so on). This

¹⁷⁴ Dorney, above n 55, 645.

¹⁷⁵ *Electronic Communications Privacy Act of 1986* 18 USC § 2702(b)(1).

¹⁷⁶ *Electronic Communications Privacy Act of 1986* 18 USC § 2707(c).

¹⁷⁷ *Electronic Communications Privacy Act of 1986* 18 USC § 2707(b)(3).

¹⁷⁸ James Sweet, 'Opting-Out of Commercial Telemarketing: The Constitutionality of the National Do-Not-Call Registry' (2003) 70 *Tennessee Law Review* 921, 931.

¹⁷⁹ Ian Ayres and Matthew Funk, 'Marketing Privacy' (2003) 20 *Yale Journal on Regulation* 77, 83.

information allows companies to make decisions and assess whether a particular individual may prove of value to them or not (for example, individual financial ability to purchase products, or qualify for a bank loan, buy a membership, and so on).¹⁸⁰

In response to this rapid growth in telemarketing, together with new technologies that both raised privacy concerns, the US Congress passed the *Telephone Consumer Protection Act* (TCPA) on 20 December 1991.¹⁸¹ The Act defined ‘telephone solicitation’ as ‘the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person’.¹⁸² This definition, however, does not include calls or messages to: (1) any person who has given prior express invitation or permission to call, (2) to person who has an established business relationship, or (3) calls or messages by a tax exempt nonprofit organisation.¹⁸³

The TCPA, however, protects consumer’s privacy by specifically prohibiting three types of calls: (1) calls using automatic dialing system or an artificial or pre-recorded voice which are directed to emergency service providers such as: emergency lines to hospitals, medical physicians, health care facilities, poison control centres, or fire fighting agencies or law enforcement agencies, guest rooms or patient rooms of hospitals, or homes (care facilities) for the

¹⁸⁰ Ibid 85.

¹⁸¹ *Telephone Consumer Protection Act of 1991* 47 USC § 227.

¹⁸² *Telephone Consumer Protection Act of 1991* 47 USC § 227(a)(4).

¹⁸³ *Telephone Consumer Protection Act of 1991* 47 USC § 227(a)(4).

elderly,¹⁸⁴ (2) calls to any residential telephone line using an artificial or pre-recorded voice without prior express consent of the called party,¹⁸⁵ and (3) using fax machine, computer or other device to send an unsolicited advertisement.¹⁸⁶

In addition, the TCPA facilitates the creation of the ‘National Do-Not-Call Registry’ database to be implemented by the Federal Communication Commission (FCC) in conjunction with the Federal Trade Commission (FTC).¹⁸⁷ The National Do-Not-Call Registry comprises a list of telephone numbers of residential and mobile phones users who object to receiving unsolicited telephone calls from the telemarketers. Accordingly, telemarketing companies are not allowed to call any number listed in the registry database, subject to certain exceptions. Telemarketers may continue to call individuals who have not placed their numbers on a do-not-call list and those with whom they have an established business relationship. Furthermore, calls regarding political and religious speech will not be subject to the do-not-call requirements since they are not considered ‘telephone solicitations’ under the TCPA.¹⁸⁸

¹⁸⁴ *Telephone Consumer Protection Act of 1991* 47 USC § 227(b)(1)(A).

¹⁸⁵ *Telephone Consumer Protection Act of 1991* 47 USC § 227(b)(1)(B).

¹⁸⁶ *Telephone Consumer Protection Act of 1991* 47 USC § 227(b)(1)(C).

¹⁸⁷ Federal Communications Commission, *Nationwide Do-Not-Call Registry* (2003) Federal Communications Commission <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-235841A1.doc> at 3 February 2010.

¹⁸⁸ *Ibid.*

In case of violations of the above provisions, the TCPA grants individuals a private right of action for damages and injunctive relief.¹⁸⁹ The parties that violate the above provisions of the TCPA may be sued directly by the recipients of such calls and may be enjoined from making future calls and/or required to pay for the actual monetary loss incurred by the call recipient at a minimum of USD 500.¹⁹⁰ With regard to businesses found to have solicited consumers on the Do-Not-Call Registry, the Act provides an affirmative defence that the business has taken due care to establish and implement reasonable practices and procedures to prevent telephone solicitations in violation of the Do-Not-Call Registry regulations.¹⁹¹

It is worth mentioning that telemarketers challenged the above Act by arguing that its provisions and regulations violate the *First Amendment* of the *US Constitution* which guarantees the freedom of commercial speech. In *Destination Ventures Ltd v Federal Communications Commission*,¹⁹² the Ninth Circuit Court dismissed a claim by *Destination* that the ban of unsolicited faxes containing advertising under the TCPA is unconstitutional because it impermissibly regulated commercial speech, thus violating the *First Amendment*. The Ninth Circuit found that for the government to regulate commercial speech without violating the *First Amendment*, it must comply

¹⁸⁹ Paul J Batista, 'The Perils of Telemarketing under the Telephone Consumer Protection Act: Sending Unsolicited Faxes Costs Dallas Cowboys \$1.73 Million, Leaves Dallas Mavericks Under Full Court Pressure' (2003) 25 *Hastings Communications and Entertainment Law Journal* 231, 235.

¹⁹⁰ *Telephone Consumer Protection Act of 1991* 47 USC § 227(b)(3).

¹⁹¹ Steven Masur, 'Mobile Phone Text Message Spam: Building a Vibrant Market for Mobile Advertising while Keeping Customers Happy' (2007) 7 *Virginia Sports & Entertainment Law Journal* 41, 48.

¹⁹² See *Destination Ventures, Ltd v Federal Communications Commission*, 46 F 3d 54 (9th Cir, 1995).

with the four-part test set forth by the Supreme Court in *Central Hudson Gas and Electric Corp v Public Service Commission*.¹⁹³ The four-part test comprises the following: (1) the commercial speech must be a lawful activity and must not be misleading, (2) the government must have a substantial interest in regulating the speech, (3) the regulation would serve to directly advance that interest, and (4) the regulation may not be more extensive than is necessary to protect the government interest.

Based on the above test, the Ninth Circuit in *Destination v FCC* determined that the ban on unsolicited fax advertisements contained in the TCPA did not violate the free speech provisions of the *First Amendment*.¹⁹⁴ The courts, in similar cases,¹⁹⁵ have concluded that privacy of the home is a significant interest and recognise that the telephone is a uniquely invasive technology that allows those soliciting for business to come into the home. The courts determined that the regulations are tailored to reasonably for the goal of protecting privacy.¹⁹⁶

7.4.2.3 Children's Online Privacy Protection Act of 1998

The *Children's Online Privacy Protection Act of 1998* (COPPA) is one of the most significant laws to protect the privacy of children under the age of 13 in the online environment.¹⁹⁷ The Act has three main objectives: (1) to enhance parental involvement in order to protect the privacy of children in online

¹⁹³ See *Central Hudson Gas and Electric Corp v Public Service Commission*, 447 US 557, 561 (1981).

¹⁹⁴ Batista, above n 189, 239.

¹⁹⁵ See *Moser v FCC*, 46 F 3d 970, 971 (9th Cir, 1995).

¹⁹⁶ Patricia Pattison and Anthony F. McGann, 'General Law Division: State Telemarketing Legislation: A Whole Lotta Law Goin' on!' (2003) 3 *Wyoming Law Review* 167, 193.

¹⁹⁷ *Children's Online Privacy Protection Act of 1998* 15 USC § 6501.

environment, (2) to help protect the safety of children in the online environment (such as, chat rooms, home pages, and pen-pal services) where children may make public postings of identifying information that may be collected online, and (3) to limit the collection of personal information from children without parental consent.¹⁹⁸ The Act requires that ‘operators’¹⁹⁹ of websites directed to children under 13 or those who knowingly collect personal ‘information’²⁰⁰ from children under 13 on the internet must meet the following five key requirements: (1) notice,²⁰¹ (2) parental consent,²⁰² (3) parental review,²⁰³ (4) limits on the use of games and prizes,²⁰⁴ and (5) confidentiality, security and integrity of personal information collected from children.²⁰⁵

With regard to the ‘notice’ requirement, an operator of online service directed to children must provide notice about what information is being collected from children, how it uses this information, and to whom, if anyone,

¹⁹⁸ Klosek, above n 99, 141.

¹⁹⁹ An ‘Operator’ means: ‘any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service commerce ... but does not include any nonprofit entity...’. See 15 USC § 6501(2)(A).

²⁰⁰ ‘Personal Information’ means ‘individually identifiable information about an individual collected online, including: (a) a first name and last name, (b) a home or other physical address including street name and name of a city or town, (c) an e-mail address, (d) a telephone number, (e) a Social Security Number, (f) any other identifier that the Commission determines permits the physical or online contacting of a specific individual, and (g) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifiers listed in this paragraph’. See 15 USC § 6501(8).

²⁰¹ *Children's Online Privacy Protection Rule*, 16 CFR § 312.4 (1999).

²⁰² *Children's Online Privacy Protection Rule*, 16 CFR § 312.5 (1999).

²⁰³ *Children's Online Privacy Protection Rule*, 16 CFR § 312.6 (1999).

²⁰⁴ *Children's Online Privacy Protection Rule*, 16 CFR § 312.7 (1999).

²⁰⁵ *Children's Online Privacy Protection Rule*, 16 CFR § 312.8 (1999).

it discloses that information.²⁰⁶ Such a notice must be placed in a clear and prominent place on the home page (of the website), or on each section where children provide, or asked to provide personal information of the website or online service.²⁰⁷

'Parental consent' requires that an operator must obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children.²⁰⁸ A consent granted to an operator for one single practice, such as for collection of personal information, does not mean that the parents are consenting for disclosure to third parties.²⁰⁹ In order to comply with this requirement, an operator must make all reasonable efforts to obtain verifiable parental consent, taking into account available technology.²¹⁰ This requirement grants parents a powerful right to veto primary collection, primary use, secondary use, and even maintenance of information. This strong right is not available to individuals under any other US privacy protection regulations.²¹¹

To comply with the third requirement of 'parental review', an operator must provide a means for a parent to review information that has been collected and a means for the parent to contact the operator to prohibit further use or

²⁰⁶ Laurel Jamtgaard, 'Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act' (2000) 16 *Computer High Technology Law Journal* 385, 388.

²⁰⁷ *Children's Online Privacy Protection Rule*, 16 CFR § 312.4(b) (1999).

²⁰⁸ *Children's Online Privacy Protection Rule*, 16 CFR § 312.5(a)(1) (1999).

²⁰⁹ *Children's Online Privacy Protection Rule*, 16 CFR § 312.5(a)(2) (1999).

²¹⁰ *Children's Online Privacy Protection Rule*, 16 CFR § 312.5(b)(1) (1999).

²¹¹ Anita L Allen, 'Minor Distractions: Children, Privacy and E-Commerce' (2001) 38 *Houston Law Review* 751, 763.

maintenance of the child's personal information.²¹² Further, an operator must provide parents with an option at any time to refuse to permit the operator's further use or further online collection of personal information, and to direct the operator to delete the child's personal information.²¹³

The fourth requirement, 'limits of the use of games and prizes', prohibits the website operator from collecting, more than 'reasonably necessary' personal information about children in order for them to participate in games and prizes.²¹⁴ However, the term of 'reasonably necessary' may be questionable as regards what information would be considered 'reasonably necessary'.²¹⁵ Finally, a website operator must maintain the confidentiality, security and integrity of personal information collected from children.²¹⁶

Despite the fact that the above Act addresses one of the most significant issues of privacy —children's privacy — there are a number of shortcomings in this Act. First, the mechanisms available for parents to provide their consent are inadequate to protect children's privacy because children can simply fabricate information to access websites. Websites can also state that they do not sell products or services to children. Second, giving a definition of the child as a 'person under the age of 13' is arbitrary and unjustified, as persons over the age of 13 may also require online privacy protection.²¹⁷

²¹² Jamtgaard, above n 206, 389.

²¹³ *Children's Online Privacy Protection Rule*, 16 CFR § 312.6 (1999).

²¹⁴ *Children's Online Privacy Protection Rule*, 16 CFR § 312.7 (1999).

²¹⁵ Jamtgaard, above n 206, 389.

²¹⁶ *Children's Online Privacy Protection Rule*, 16 CFR § 312.8 (1999).

²¹⁷ William G Staples (ed), *Encyclopedia of Privacy* (2007) vol 1, 95.

The Act authorises the Federal Trade Commission (FTC) to issue a rule for the enforcement of COPPA provisions.²¹⁸ The FTC adopted its final Children's Privacy Protection Rule in April 2000; it became effective six months thereafter, the timespan allocated in order to provide websites with enough time to enable them to comply with the Rule.²¹⁹ The COPPA also provides that the regulatory framework can be avoided by following industry self-regulatory guidelines that are approved by the FTC.²²⁰ Before approving such guidelines, the FTC must determine whether they meet the requirements of the FTC regulations.²²¹ Consequently, the first case of its kind to reflect concerns for children's privacy online was the civil suit brought by the FTC against website *Geocities*.²²² The FTC charged *GeoCities* with misrepresenting and deceptive practices when *GeoCities* collected personal identifying information (e-mails, postal addresses, member interest areas, and demographic data including income, educations, gender, marital status and occupation) about its members and assured to them that this information would not be released to anyone without the member's permission. In fact, this information was disclosed to third parties who used

²¹⁸ *Children's Online Privacy Protection Act of 1998* 15 USC § 6501 § 6505 (a).

²¹⁹ Federal Trade Commission, *Children's Online Privacy Protection Rule, 16 CFR Part 312* (2010) FTC <http://www.ftc.gov/privacy/privacyinitiatives/COPPARule_2005SlidingScale.pdf> at 4 February 2010.

²²⁰ *Children's Online Privacy Protection Act of 1998* 15 USC § 6503

²²¹ *Children's Online Privacy Protection Act of 1998* 15 USC § 6503(b)(3).

²²² *Federal Trade Commission (FTC) v GeoCities*, File No 982 3015, Docket No C-3850, 13 August 1998.

it to target members for solicitations beyond those agreed to by the member.²²³

The case was settled when the FTC and *GeoCities* reached an agreement that *GeoCities* would refrain from misleading consumers, including children, about its privacy information practices, such as the purpose of the collection and the uses of their personal identifying information. Further, the settlement required that *GeoCities* place on its website a clear and prominent 'privacy notice', informing consumers what information was being collected and for what purpose, to whom it would be disclosed, and how consumers could access and remove the information. In addition, the settlement imposed on *GeoCities* a requirement to obtain parental consent before collecting personal information from children 12 and under. *GeoCities* agreed to notify its members and to provide them with an opportunity to have their information deleted from *GeoCities* and any third parties' databases. Finally, *GeoCities* also agreed to provide, for five years, a clear and prominent hyperlink within its 'privacy notice' directing visitors to the FTC's website, enabling users to view educational material on consumer privacy.²²⁴

The above settlement and similar cases,²²⁵ may support the central question of this research of whether self-regulatory guidelines are suitable for privacy

²²³ Federal Trade Commission, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case* (Press release) 13 August 1998 (1998) FTC <<http://www.ftc.gov/opa/1998/08/geocitie.shtm>> at 5 February 2010.

²²⁴ Ibid.

²²⁵ See *Federal Trade Commission (FTC) v Toysmart.com LLC, and Toysmart.com Inc*, Civil Action No 00-11341-RGS, FTC File No X000075, 21 July 2000. In this case, the FTC sued the failed website Toysmart.com for deceptively offering for sale personal information of website visitors. Toysmart collected details about their customers, including names, addresses, billing information, preferences,

protection or not. From the FTC practical procedures it seems evident that self-regulation not government intervention will play a significant and effective role in protecting and maintaining individual privacy in the context of the area of telecommunications. However, the suitability and effectiveness of the self-regulation approach shall be examined at later stage of this research.

7.4.3 Privacy Laws Concerning US Financial Sector

The financial services sector is one of the most regulated sectors in the United States.²²⁶ The stringent regulation of this business sector is based on the protection of individual privacy.²²⁷ The US Congress has enacted several pieces of legislation to address the concern for individual privacy. This section explores the details of the laws adopted to deal with the privacy issue in the US.

7.4.3.1 Gramm-Leach-Bliley Act (GLBA) of 1999

In 1999, the US Congress passed the *Financial Services Modernization Act of 1999*, which also known as the *Gramm-Leach-Bliley Act of 1999 (GLBA)*.²²⁸ Congress enacted the GLBA to create a balance between the need for increased competition in the financial services and to protect nonpublic

and birth dates. Their privacy policy promised that 'personal information will never be shared with third parties'. In May 2000, Toysmart.com closed their doors and began to liquidate their assets-including lists of customers – in violation of their own policy.

²²⁶ Schwartz and Reidenberg, above n 143, 23.

²²⁷ Virginia Boyd, 'Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization' (2006) 24(3) *Berkeley Journal of International Law* 939, 943.

²²⁸ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809.

personal information in the financial services sector.²²⁹ Title V of the GLBA contains a number of privacy provisions designed to protect the privacy of ‘nonpublic personal information’²³⁰ that consumers provide to financial institutions.²³¹ The privacy provisions under the GLBA consist of four important requirements. The first is ‘notice’. The financial institutions must provide ‘privacy notice’ in order to disclose any non-public personal information to non-affiliated third party.²³² The idea of ‘privacy notice’ under the GLBA is to convey information that is critical to an individual’s decision-making concerning the use of his/her personal information.²³³

The second requirement refers to ‘choice’, which requires the financial institutions to grant consumers the option of preventing their personal information from being shared with a non-affiliated third party.²³⁴ The financial institution must provide an ‘opt-out’ option for their consumers

²²⁹ Jim Hietala, 'Managing Information Privacy' (2008) 21(3) *Bank Accounting & Finance* 41. For example, in the period from January to August 2007, security breaches involving financial institution occurred at the following institutions (among others): (1) Aflac: 152,000 names, addresses, insurance records, (2) Bank of Scotland: 62,000 mortgage account numbers, names, addresses, dates of birth, (3) Fidelity National Information Services: 2.3 million consumer records, credit card and bank account information, (4) JP Morgan Chase: 47,000 Social Security Numbers (SSNs) and account numbers, (5) Merrill Lynch: 33,000 SSNs, (6) Western Union: 20,000 names and credit card numbers: 41–2.

²³⁰ The term ‘nonpublic personal information’ means ‘personally identifiable financial information (i) provided by a consumer to a financial institution. (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution’: *Gramm-Leach-Bliley Act of 1999* 15 USC § 6809(4)(A). Pub L No 106-102, § 509(4)(a), 113 Stat 1443.

²³¹ These provisions are found under Title V ‘Privacy’ of the *Gramm-Leach-Bliley Act of 1999*, Pub L No 106-102, §§ 501–509, 521–527. *Gramm-Leach-Bliley Act of 1999* Pub L No 106-102, 113 Stat 1443.

²³² *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809 Pub L No 106-102, § 502(a), 113 Stat 1443.

²³³ Edward J Janger and Paul M Schwartz, 'The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules' (2001) 86 *Minnesota Law Review* 1219, 1225.

²³⁴ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809, Pub L No 106-102, § 502(b), 113 Stat 1443.

exercising the choice requirement.²³⁵ As has been discussed earlier (Chapter Four), ‘opt-out’ means an implied consent given by the individual unless he/she objects to the use of his/her personal information by the financial institution. The individual in the opt-out option is responsible for notifying the financial institution not to use, and/or share his/her personal information. The ‘opt-in’ option is the opposite. Under this option the financial institution must obtain an explicit consent from an individual in order to use or share his/her for purposes other than that for which it was originally collected.

The financial industry has generally favoured a default rule of allowing sharing of information, with customers able to opt out if they choose to limit or prevent sharing of information.²³⁶ However, privacy advocates argue that opt-out option puts too much of a burden on consumers to protect their privacy, while the opt-in option burdens everyone who wants the advantages offered by the use of shared information and imperils the viability of the businesses that provide those advantages.²³⁷

The third requirement is called ‘security and confidentiality’. The GLBA requires that financial institutions implement administrative, physical, and technical standards to protect against loss and unauthorised access,

²³⁵ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809, Pub L No 106-102, § 502(b), 113 Stat 1443.

²³⁶ Peter P Swire, 'The Surprising Virtues of the New Financial Privacy Law' (2001) 88 *Minnesota Law Review* 1263, 1267.

²³⁷ Kent Walker, 'The Cost of Privacy' (2001) 25 *Harvard Journal of Law & Public Policy* 87, 116.

destruction, use, or disclosure of information.²³⁸ These standards are: (1) to insure the security and confidentiality of customer records and information, (2) to protect against any anticipated threats of hazards to the security or integrity of such records, and (3) to protect against unauthorised access to or use of such records or information which could result in substantial harm or inconvenience to any customer.²³⁹

The fourth requirement for guarantee of the privacy of information under the Act is 'enforcement'. The GLBA requires eight federal agencies to enforce the privacy provisions and regulations within each agency's jurisdiction.²⁴⁰ The right of enforcement under the GLBA is assigned to these federal agencies rather than to consumers whose privacy has been violated.²⁴¹

However, the requirement of enforcement of financial privacy regulation under this Act is difficult to achieve because all eight federal agencies must adopt similar regulations, standards and safeguards in order to comply with the GLBA's information privacy practices' requirements.²⁴² For example, the Security and Exchange Commission (SEC), National Trade Union Administration (NTUA), and Commodities Future Trading Commission (CFTC) can enforce privacy regulations against businesses in their

²³⁸ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809, Pub L No 106-102, § 502(a), 113 Stat 1443.

²³⁹ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809, Pub L No 106-102, § 501(b), 113 Stat 1443.

²⁴⁰ These agencies are: (1) Federal Reserve Board (FRB), (2) Office of Thrift Supervision (OTS), (3) National Credit Union Administration (NCUA), (4) Federal Deposit Insurance Corporation (FDIC), (5) Comptroller of the Currency (OCC), (6) Security and Exchange Commission (SEC), (7) Federal Trade Commission (FTC) and, (8) Commodity Futures Trading Commission (CFTC).

²⁴¹ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809, Pub L No 106-102, § 505, 113 Stat 1443.

²⁴² Boyd, above n 228, 950.

jurisdiction, while the Federal Trade Commission can use its powers to enforce prohibitions of unfair or deceptive trade practices against any financial institution that is not subject to one of the above agencies.²⁴³ This means that different agencies have different rules and authorities to regulate financial transactions.

In summary, the privacy requirements within the GLBA provide to a great extent the most comprehensive privacy legislation in US history. The GLBA gives consumers, for the first time, an absolute right to know whether their financial institution plans to sell, disclose or share their personal financial information with third parties, whether or not these parties are affiliated or non-affiliated third parties.²⁴⁴ In addition, the impact of these GLBA privacy requirements has spread beyond the shores of the United States. They have been studied and adopted as a model by international organisations in their attempts draft recommendations for privacy protection guidelines for members. The Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (as previously discussed in Chapter Two) provides one such example as its Guidelines have adopted incorporated the similar requirements for the protection of individual privacy.). It is, however, up to each member country to decide whether to adopt these.

²⁴³ Swire, 'The Surprising Virtues of the New Financial Privacy Law', above n 236, 1272.

²⁴⁴ Neal R Pandozzi, 'Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation' (2001) 55 *University of Miami Law Review* 163, 164.

7.4.3.2 Fair Credit Reporting Act of 1970

The *Fair Credit Reporting Act of 1970*²⁴⁵ (FCRA) –as a new title to the *Consumer Credit Protection Act of 1968*–aims to ensure that credit reporting agencies²⁴⁶ treat information in consumer credit reports²⁴⁷ prepared by them in a manner that is ‘fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilisation’ of the consumer’s credit information.²⁴⁸ It is also the first legislation, designed to regulate the personal information market in the United States, a market that includes credit bureaux,²⁴⁹ investigative reporting²⁵⁰ companies, and other organisations whose business is the collection and reporting of personal information.²⁵¹

The FCRA requires the uses of personal information in consumer reports obtained from a consumer reporting agencies only under certain purposes: ²⁵²

²⁴⁵ *Fair Credit Reporting Act of 1970* 15 USC § 1681. Amended in 1992.

²⁴⁶ A ‘consumer reporting agency’ is defined in 15 USC § 1681a(f) as: ‘any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports’.

²⁴⁷ The term ‘consumer reports’ are defined in 15 USC § 1681b(d) as ‘any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for: (A) credit or insurance to be used primarily for personal, family, or household purposes, (B) employment purposes, or (C) any other purpose authorised under section 604, § 1681b.

²⁴⁸ *Fair Credit Reporting Act of 1970* 15 USC § 1681(b).

²⁴⁹ There are three major credit bureaux in the United States: see (1) Equifax: <www.equifax.com>, (2) Experian: <www.experian.com>, and (3) Trans Union: <www.transunion.com>.

²⁵⁰ An ‘investigative consumer report’ (ICR) mainly includes information on character, reputation, personal characteristics, and mode of living. ICRs are compiled from personal interviews with persons who know the consumer. Since ICRs include especially sensitive information, the FCRA affords them greater protections. For instance, within three days of requesting an ICR, the requester must inform the consumer that an ICR is being compiled. The consumer also can request a statement explaining the nature and scope of the investigation underlying the ICR.

²⁵¹ Blair C Fensterstock, ‘The Public and the Fair Reporting Act’ in Theodore R Kupferman (ed), *Privacy and Publicity* (1990) 2.

²⁵² *Fair Credit Reporting Act of 1970* 15 USC § 1681(b)(a).

(1) court orders, including grand jury subpoenas, (2) applications for credit, insurance, and rentals for personal, family or household purposes, (3) employment, which includes hiring, promotion, reassignment or retention, (4) for legitimate business needs in transactions initiated by the consumer for personal, family, or household purposes, (5) account reviews when banks and other companies review credit files to determine whether they wish to retain the individual as a customer, (6) licensing, (7) child support payment determinations, and (8) law enforcement access — government agencies with authority to investigate terrorism and counter intelligence have secret access to credit reports.

The FCRA adopted three principles for the protection of personal privacy, which include: notice, choice, and access. These principles were introduced in to the FCRA by the *Fair and Accurate Credit Transactions Act of 2003* (FACTA 2003), which was adopted in 2003 to amend the FCRA.²⁵³

On the principal of 'notice', the FACTA 2003 provides that an entity that receives information from an affiliate may not use that information to make marketing solicitations without providing clear and conspicuous notice to the consumer.²⁵⁴ For example, the FACTA 2003 requires that a creditor notify a consumer when it offers her/him credit terms that are materially less

²⁵³ *Fair and Accurate Credit Transactions Act of 2003* 15 USC § 1601.

²⁵⁴ Boyd, above n 227, 952.

favourable than the most favourable terms available to a substantial proportion of consumers.²⁵⁵

On the principal of ‘choice’, FACTA 2003 gives consumers the right to prohibit the use of their personal information by affiliates for marketing purposes.²⁵⁶ For instance, consumers have the right to opt out of receiving pre-approved credit card offers to their mail.²⁵⁷ Consumers can notify credit reporting agency by phone, in this case, the opt-out request will last for two years and then expire, or the consumers can exercise the right of opt-out by submitting a signed request to the credit reporting agency, the request remains in force until the consumer informs the agency otherwise.²⁵⁸

On the principal of ‘access’, consumers have the right to access to their information and may correct, delete, or amend any inaccurate information stored in the credit reporting agencies’ files. If a dispute arises with regard to the inaccuracy of the information and this information could not be verified, the information must be deleted or removed from the consumer’s file.²⁵⁹ Further, FACTA 2003 increased consumers’ rights of access by granting consumers a right to obtain a free annual credit report from each of the three major credit reporting agencies.

²⁵⁵ Electronic Privacy Information Center, *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report* Electronic Privacy Information Center <<http://epic.org/privacy/fcra/>> at 13 February 2010.

²⁵⁶ Ibid.

²⁵⁷ Klosek, above n 99, 134.

²⁵⁸ *Fair and Accurate Credit Transactions Act* of 2003 15 USC § 1681b(e).

²⁵⁹ *Fair Credit Reporting Act* of 1970 15 USC § 1681(i).

The FCRA provides civil and criminal penalties for individuals who fail to comply with the law. The civil penalty imposes fines of ‘actual damages sustained by the consumer’ between USD 100 and USD 1000 as well as punitive damages and attorney’s fees and costs.²⁶⁰ The criminal penalties imposed under the FCRA apply to ‘any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses’.²⁶¹ Furthermore, the FTC is also authorised to enforce administrative compliance with the FCRA, issuing opinions and interpretations of the FCRA for consumer reporting agencies and users of their services, and bringing actions for enforcement of the FCRA.²⁶² However, the interpretations and opinions issued by the FTC are not substantive rules and do not have the legal effect. They are advisory in nature and represent the FTC’s view of how the FCRA should be interpreted.²⁶³

7.4.3.3 Right to Financial Privacy Act of 1978

The US Congress enacted the *Right to Financial Privacy Act of 1978*²⁶⁴ (RFPA) in response to the US Supreme Court decision in *United States v Miller*, which ruled that customers have no right to privacy (‘expectation of privacy’) in the contents of their records held by financial institutions.²⁶⁵ The Court

²⁶⁰ *Fair Credit Reporting Act* of 1970 15 USC § 1681(n).

²⁶¹ *Fair Credit Reporting Act* of 1970 15 USC § 1681(q).

²⁶² *Fair Credit Reporting Act* of 1970 15 USC § 1681(s).

²⁶³ Bonnie G Camden, 'Fair Credit Reporting Act: What You Don't Know May Hurt You' (1988) 57 *Cincinnati Law Review* 267, 272.

²⁶⁴ *Right to Financial Privacy Act of 1978* 12 USC § 3401.

²⁶⁵ See *US v Miller*, 425 US 436 (1976).

In summary, The United States sought certiorari review of a judgment from the United States Court of Appeals for the Fifth Circuit, which reversed defendant’s convictions on four counts involving an

concluded that individuals have no constitutional protection against government access to banking records belonging to individuals. This is because that when individuals voluntarily share records in the ordinary course of a business relationship with banks, they have renounced their expectation of privacy.²⁶⁶ This decision highlights the failure of the *Privacy Act of 1974* — which is supposed to govern government actions (as discussed above) — to protect financial privacy.²⁶⁷

However, in the context of financial information, government actions are regulated under the RFPA in two ways.²⁶⁸ First, the RFPA prohibits financial institutions from providing any government agency access to, or copies of, the information contained in the financial records of any customer except in three specific instances:²⁶⁹ (1) if the customer authorises such access to his/her financial records,²⁷⁰ (2) if the government has a valid subpoena or

unregistered still and failure to pay taxes, and held that the district court erred in failing to suppress bank records kept under the Bank Secrecy Act. As a result, Bureau of Alcohol, Tobacco and Firearms agents gave grand jury subpoenas issued in blank from the district court to the presidents of banks where defendant Mitchell Miller kept accounts. The banks made the documents available to the agents, which were used in their investigation of defendant and at his trial. Defendant was convicted of possessing an unregistered still, operating a distillery without bond or paying whisky taxes, possessing untaxed whiskey, and conspiring to defraud the United States of taxes. The appellate court reversed, finding that the bank records should have been suppressed. On certiorari review, the United States Supreme Court held that defendant had no legitimate expectation of privacy in his bank records because the bank was a third party to which he disclosed his affairs when he opened his accounts at the bank. Since the Fourth Amendment of the U.S. Constitution did not protect information revealed to a third party, and since records kept under the Bank Secrecy Act, did not add additional protection, the records were properly admitted into evidence. This case is considered to be a landmark in individuals' constitutional reasonable expectation of privacy in personal records held by third parties. As a result, the U.S. Supreme Court reversed the appellate court's judgment setting aside defendant's convictions and remanded the case for future proceedings on an issue that had been deferred.

²⁶⁶ Staples, above n 217, 39.

²⁶⁷ Matthew N Kleiman, 'The Right to Financial Privacy versus Computerized Law Enforcement: A New Fight in an Old Battle' (1992) 86 *Northwestern University Law Review* 1169, 1186.

²⁶⁸ Ibid 1188.

²⁶⁹ *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3403(a).

²⁷⁰ *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3402(1).

search warrant for the financial records,²⁷¹ or (3) under special circumstances, if there is a formal written request from government officials to banks who are authorised to obtain bank records.²⁷²

Second, the RFPA prohibits the transfer of financial records between federal agencies unless the agency certifies in writing that there are substantial grounds to believe that such transfer is necessary to enforce a law, or for counterintelligence activity, investigation or analysis related to international terrorism within the jurisdiction of the receiving government agency of the financial records.²⁷³

The second prohibition is important in relation to the protection of individual financial privacy. The RFPA regulates only disclosures to the federal agencies and their officials; it does not regulate the sharing of financial records with private businesses, or with state governments.

Furthermore, the RFPA requires that government agency must notify individual that his/her financial records will be requested, and provide him/her with substantial grounds to justify the request. The government agency must explain to customers the specific nature of these grounds.²⁷⁴ In addition, a federal government agency must ensure that the customer has a

²⁷¹ *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3402(2) (3) (4).

²⁷² *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3402(5).

²⁷³ *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3412(a).

²⁷⁴ *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3405(2).

fair opportunity to object and challenge any request of his/her financial records before transfer or sharing can be made.²⁷⁵

The RFPA imposes civil penalties against any federal government agency for violation its provisions. The injured person may seek compensation for: actual damages from the government (US), and/or punitive damages, as a result of the transferring or sharing his/her financial records, and any costs and fees in the case of any successful action would be against the government. However, the minimum damages awarded to a customer in the case of violation of the RFPA provisions are USD 100.²⁷⁶

In summary, the RFPA is clearly a significant step, along with the *Privacy Act of 1974*, toward providing a clearly needed right of customers to protect personal financial records from government ‘invasions’ of privacy;²⁷⁷ however, judicial interpretations have failed to use the tools in these laws to provide such protection in the context of financial information, as illustrated in the *United States v Miller* case.²⁷⁸ Further, the RFPA has many exceptions. The most noteworthy is the *Bank Secrecy Act of 1970*, which is to be discussed in the next section.

²⁷⁵ *Right to Financial Privacy Act of 1978* 12 USC § 3401, § 3410.

²⁷⁶ *Right to Financial Privacy Act of 1978* 12 USC § 3417.

²⁷⁷ Roy L Moore, 'The 1978 Right to Financial Privacy Act and U.S. Banking Law' in Theodore R Kupferman (ed), *Privacy and Publicity* (1990) 208.

²⁷⁸ Keiman, above n 267, 1191.

7.4.3.4 Bank Secrecy Act of 1970

The US Congress passed the *Currency and Foreign Transactions Reporting Act*, commonly known as the *Bank Secrecy Act of 1970* (BSA 1970)²⁷⁹ to help government agencies to detect and prevent money laundering, tax evasion, embezzlement, drug related transactions and illegal activities. The method, here, is to create an audit trail by identifying the source and dollar amount of any transaction consisting of currency or other monetary instruments coming into or leaving the United States, and subsequently the apprehension and prosecution of individuals involved in any of the above activities.²⁸⁰ Therefore, the BSA requires individuals, banks, and other financial institution to report information with the US Department of the Treasury (US Treasury). The information includes: name, address and occupation, in addition to information related to financial transactions.²⁸¹ This information is to be collected and transmitted, without the knowledge or consent of customers, whenever the financial institution detected suspicious activity. For example, financial institutions must report each deposit, withdrawal, exchange of currency, or other payment or transfer which involves a transaction in currency of more than USD10, 000 in one day.

However, the widespread tracking of individual finances mandated by the BSA 1970 has been constitutionally challenged. In the distinguished case of *California Bankers' Association v Schulz*, the BSA 1970 was challenged on the

²⁷⁹ *Bank Secrecy Act of 1970* 31 USC § 1951.

²⁸⁰ Staples, above n 217, 43.

²⁸¹ Federal Financial Institution Examination Council, *Bank Secrecy Act/ Anti-Money Laundering: Examination Manual* (2006) Federal Financial Institution Examination Council <http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf> at 25 February 2010.

constitutional grounds of freedom of association, unreasonable search and seizure, and the right against self-incrimination, as guaranteed by the First, Fourth and Fifth Amendments of the *US Constitution*.²⁸² The Supreme Court, however, affirmed the constitutionality of the *Bank Secrecy Act of 1970* as it did not impose unreasonable reporting requirements on banks nor did it violate any rights of the plaintiff.

In sum, it appears that the above US privacy laws were mainly enacted to address the issue of privacy for specific industries and sectors, rather than providing comprehensive and detailed legislation for regulation and protection of privacy. It seems that the driving force behind the formation of the current US privacy landscape is mainly related to the preservation of the specific interests of businesses rather than the interests of privacy itself. For example, in the telecommunications sector, the passage of the ECPA depended on the belief of service providers that consumers would not use their services unless the telecommunications industry maintained an acceptable level of individual privacy. Furthermore, in the financial sector, the enactment of the GLBA was mainly based to the need by business to accept some limitations on their personal information practices and provide certain right to individuals in order to achieve sector's goal of modernisation and consolidation.²⁸³

²⁸² *California Bankers Association v Shultz*, 416 US 21 (1974).

²⁸³ Priscilla M Regan, 'The United States' in James B Rule and Graham Greenleaf (eds), *Global Privacy Protection: the First Generation* (2008) 76–7.

As illustrated above, the US Congress enacted laws that outline the general issues and principles of privacy, but leave the specific details to be implemented through rules and regulations to be adopted by government agencies. One of the most effective regulatory agencies to address privacy concerns in the context of information and communications technologies is the US Federal Trade Commission (FTC). The following section provides a closer look into the role of the FTC toward privacy protection, and then examines its adopted approach in this regard.

7.5 The Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) was established in 1914 by the *Federal Trade Commission Act* (FTCA). It was adopted as a regulator to prevent unfair competition and unfair practices in trade and commerce.²⁸⁴ Over the time, the FTC has become the only US federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy.²⁸⁵ However, in the light of rapid developments in information and communications technology, the FTC plays a major role to regulate and enforce its regulations in order to protect individual privacy in this context. On the issue of privacy, the FTC states:²⁸⁶

Privacy is a central element of the FTC's consumer protection mission. In recent years, advances in computer technology have made it possible for details information about people to be compiled and shared more easily and

²⁸⁴ *Federal Trade Commission Act* 15 USC §§ 41-58.

²⁸⁵ Federal Trade Commission, *About the Federal Trade Commission* (2009) Federal Trade Commission <<http://www.ftc.gov/ftc/about.shtm>> at 26 February 2010.

²⁸⁶ Federal Trade Commission, *Privacy Initiatives: Introduction* Federal Trade Commission <<http://www.ftc.gov/privacy/index.html>> at 26 February 2010.

cheaply than ever.... At the same time, as personal information becomes more accessible, each of us- companies, associations, government agencies, and consumers- must take precautions to protect against the misuse of our information.

The FTC has the authority mandated by FTCA to issue regulations and rules it deems appropriate to protect individual privacy in many different sectors. In the financial sector, the FTC and in accordance with the *Gramm-Leach-Bliley Act*²⁸⁷ has issued the 'Financial Privacy Rule: 16 CFR Part 313' to govern the collection and disclosures of customers' personal information by financial institutions.²⁸⁸ The *Financial Privacy Rule* requires financial institutions to provide customers a privacy notice that accurately explains the financial institution's information collection and sharing practices. Further, the financial institutions and other entities that receive personal financial information from a financial institution may be limited in their ability to use that information.²⁸⁹ For example, in the matter of *Nations Title Agency Inc, Nations Holding Company, and Christopher Likens* (respondents), the FTC have found that respondents have violated the Financial Privacy Rule (16 CFR Part 313). The respondents provided a variety of financial services (for example, home finance, refinance mortgages, and real estate settlements services,) and were involved in a number of personal information practices including, but not limited to, consumer names, social security numbers, bank and credit card numbers, mortgage information, loan application, income and

²⁸⁷ *Gramm-Leach-Bliley Act of 1999* 15 USC §§ 6801-6809.

²⁸⁸ Federal Trade Commission, 'Privacy of Consumer Financial Information: 16 CFR Part 313' (2000) 65(101) *Federal Register* 33646.

²⁸⁹ Federal Trade Commission, *The Gramm-Leach-Bliley Act: The Financial Privacy Rule* FTC <http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html> at 3 March 2010.

credit histories. However, the FTC believed that the respondents failed to take reasonable and appropriate security measures to protect this information. The respondents failed to: (1) assess risks to the information they obtained, (2) adopt reasonable policies and procedures, (3) implement anti-virus programs to common website attacks, (4) employ reasonable safeguards to detect and respond to unauthorised access to personal information, and (5) establish reasonable oversight measures for treating personal information by third parties.²⁹⁰

Consequently, the FTC found the respondents in breach of the Financial Privacy Rule when a hacker was able to attack and access personal information stored on the respondents' networks. The company's privacy policy contained false and misleading statements regarding the measures implemented to protect consumers' personal information.²⁹¹

Another example of the FTC authority on personal privacy can be found under the *Fair Credit Reporting Act*.²⁹² In *FTC v Rental Research Services (RRS)*,²⁹³ the FTC found that the defendant RRS failed to provide reasonable and appropriate standards to protect consumers' personal information. The RRS was selling tenant screening reports online to businesses and

²⁹⁰ Federal Trade Commission, *In the Matter of Nations Title Agency Inc, Nations Holding Company, and Christopher M Likens*, File No 052 3117, Docket No C-4161 (19 June 2006) Federal Trade Commission <http://www.ftc.gov/os/caselist/0523117/0523117NationsTitle_Complaint.pdf> at 3 March 2010

²⁹¹ Ibid.

²⁹² *Fair Credit Reporting Act* of 1970 15 USC § 1681.

²⁹³ Federal Trade Commission, *United States of America (for the Federal Trade Commission) v Rental Research Services Inc, a corporation, and Lee Mikkelsen, individually and as an officer of the corporation*. FTC File No 072 3228 (5 March 2009) FTC <<http://www.ftc.gov/os/caselist/0723228/090305rrscmpt.pdf>> at 3 March 2010.

individuals. These reports containing names, social security numbers, date of birth, bank and credit card account numbers and credit histories. On one occasion, identity thieves, claiming to be a person who an actual person is operating a legitimate business, filled in an online application with RRS using publicly-available information. The thieves provided a name, a business name, number of years in business, a physical address, a hotmail (e-mail address), a mobile number, fax number and statement that the individual sought consumer reports for those renting a 150 unit property that the person owned. The RRS approved the application without seeking any further information or documentation, or performing further investigation. The RRS then e-mailed a login ID and password to the hotmail address on the application. These credentials gave the identity thieves unlimited, online access to consumer reports, which they used to purchase at least 318 consumer reports. As a result, many consumers contacted RRS claiming that their identities had been stolen by identity thieves.

The RRS agreed to settle with the FTC for its violation of the FCRA provisions. The FCRA prohibits a consumer reporting agency (RRS) from furnishing a consumer report except for specific 'permissible purposes'. In this case, the RRS furnished almost 318 consumer reports to persons who did not have a permissible purpose to obtain a consumer report. The RRS violated Section 604 the FCRA.²⁹⁴ It also violated Section 607(a) of the FCRA which requires every reporting agency to maintain reasonable

²⁹⁴ *Fair Credit Reporting Act* of 1970 15 USC § 1681b, Sec 604.

procedures to minimise the furnishing of consumer reports. The RRS failed to employ reasonable and appropriate standards to maintain the security of personal information collected by RRS to sell to its customers. RRS failed to: (1) verify or authenticate the identities and qualifications of prospective subscribers, or (2) to monitor or otherwise identify unauthorised subscriber activity.

Furthermore, with respect to children's online privacy, the FTC has brought many legal actions against businesses, such as *GeoCities* and *Toysmart.com*, in order to protect individual privacy based on the *Children's Online Privacy Protection Rule* issued by the FTC.²⁹⁵

The rule-making and enforcement authority of the FTC described above has given the FTC an important role to shape the type of regulation of privacy in the United States. In 1998, the FTC has issued an important report to US Congress regarding online privacy which contained remarkable conclusions.²⁹⁶ First, it concluded that industry had not been fully successful in implementing *Fair Information Practices* (FIPs) (which has been discussed in earlier in the chapter). Second, the FTC report called for legislation to address the specific concerns of children's privacy only. These conclusions were based on a comprehensive survey conducted by the FTC on a number of businesses that have online presence. The survey shows that 85 per cent of 1400 websites examined collect personal information from customers.

²⁹⁵ *Children's Online Privacy Protection Rule*, 16 CFR, § 312.

²⁹⁶ Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) Federal Trade Commission <<http://www.ftc.gov/reports/privacy3/priv-23a.pdf>> at 4 March 2010.

However, only 14 per cent of those websites placed any notice with respect to their information practices.²⁹⁷

With respect to websites targeting children, the survey found that 89 per cent of the surveyed websites collected personal information from children. While 54 per cent of those websites provided some form of disclosure of their practices only 23 per cent of the websites asked children to seek parental permission before providing personal information.²⁹⁸

In spite of the conclusion reached by the FTC in the 1998 Report to Congress that industry may not be effective and responsible to implement privacy protection guidelines, the FTC — in the 1999 report to Congress — concluded that comprehensive legislation to address online privacy is not recommended, and that ‘self-regulation is the least intrusive and most efficient means to ensure privacy protection online’.²⁹⁹ The report, entitled ‘Self-regulation and Privacy Online’, reached this conclusion after examining many of the self-regulatory initiatives implemented by the private sector. Although, these initiatives are beyond the scope of this study, the FTC believed that these initiatives reflected substantial effort and commitment by the private sector to fair information practices.³⁰⁰

Nevertheless, the FTC noted in this report that with the advancement of information and communications technology, the private sector faces a

²⁹⁷ Ibid.

²⁹⁸ Ibid.

²⁹⁹ Federal Trade Commission, *Self-Regulation and Privacy Online* (1999) Federal Trade Commission <<http://www.ftc.gov/os/1999/07/privacyonlinetestimony.pdf>> at 4 March 2010.

³⁰⁰ Ibid.

number of substantial challenges. In this context, the FTC recommended that ‘industry group must continue to encourage widespread adopting of fair information practices’, ‘focus its attention on the substance of website information practices, ensuring that businesses adhere to the core privacy principles’, and that ‘industry must work together with government and consumer groups to educate consumers about privacy protection in the new technology’.³⁰¹

In sum, the FTC with the support of the US government believed that implementing comprehensive legislation for privacy was not necessary in order to obtain the desired protection. It believed that industry self-regulation is the most suitable approach to protect privacy, and that the private sector has the main responsibility for ensuring this protection. However, some privacy advocates argued that the self-regulation is ineffective and inadequate, and the only way to secure individual privacy is for the US Congress to legislate comprehensive privacy legislation. Both sides of the argument are examined in the following sections:

7.5.1 The US Self-Regulation Approach to Privacy Protection

The US approach to privacy protection, as illustrated above, is a piecemeal approach. This approach stems from the US view of privacy as a property right rather than an absolute human right. The view of privacy as a property right, however, leads to the use of an approach of self-regulation, where a balance must be made between an individual’s desire to maintain his or her

³⁰¹ Ibid.

privacy,³⁰² and the benefits gained from the free flow of information, and restrictions on the government use of personal information.³⁰³ The justification for this approach is based on several arguments. First, comprehensive legislation by government would interfere with the flow of consumer information that enables businesses to provide products and services that cater to the needs and wants of their customers, and that the introduction of such legislation would result in decreased consumer choice and also minimise competition.³⁰⁴ Second, self-regulation advocates argue that comprehensive legislation to address privacy issues is unnecessary because consumers themselves who are concerned about privacy issues will force businesses to implement good privacy practices.³⁰⁵ In addition, companies may realise the significance of privacy protection in maintaining a consumer base and will adopt privacy policy as part of their overall marketing effort to develop brand reputation and an image of quality service.³⁰⁶ Third, self-regulation advocates also argue that privacy concerns in the information and communications technology are still indistinguishable, and have not been clearly identified. The rapidly changing nature of the technologies involved makes it difficult for policy makers to enact privacy laws regulating every newly invented technology. Consequently, these

³⁰² Cody, above n 98, 1202.

³⁰³ Schwartz and Reidenberg, above n 144, 6.

³⁰⁴ Eve M Caudill and Patrick E Murphy, 'Consumer Online Privacy: Legal and Ethical Issues' (2000) 19(1) *Journal of Public Policy and Marketing* 7, 11.

³⁰⁵ Peter P Swire, 'Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information' in 'Privacy and Self-Regulation in the Information Age' (US Department of Commerce, 1997) available at: <http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm>.

³⁰⁶ Scott Foster, 'Online Profiling is on the Rise: How Long until the United States and the European Union lose Patience with Self-Regulation' (2000) 41 *Santa Clara Law Review* 255, 267.

advocates argue that it would be premature to enact any kind of comprehensive regulation concerning information privacy in this context.³⁰⁷

The above arguments, however, were not good enough to convince privacy advocates to support the self-regulation approach. Privacy advocates argue that self-regulation is inadequate and ineffective, and thus the only way that consumers can achieve an acceptable level of privacy protection is to create comprehensive legislation that effectively secures consumer privacy rights and creates measures and standards by which consumers may assert those rights.³⁰⁸

This argument is based on two major factors: the voluntary nature of industry compliance, and the degree of consumer knowledge and control of information collection and use.³⁰⁹ In relation to the first factor, privacy advocates fear that under a voluntary system, self-regulation will not be strict nor consistent enough due to noncompliance and may in practice end up resembling an unregulated market.³¹⁰ As discussed earlier, the noncompliance concern was identified in the FTC survey as early as 1998, when it found a large number of websites had not been fully recognised the privacy principles of fair information practice.

³⁰⁷ Joann M Wakana, 'The Future of Online Privacy: A Proposal for International Legislation' (2003) 26 *Loyola of Los Angeles International & Comparative Law Review* 151, 164.

³⁰⁸ Shaun A Sparks, 'The Direct Marketing Model and Virtual Identity: Why the United States should Not Create Legislative Controls on the Use of Online Consumer Personal Data' (2000) 18 *Dickinson Journal International Law* 517, 542.

³⁰⁹ Marc Rotenberg, 'Self-regulation Won't Work', *USA Today* (McLean, VA), 7 July 1998, 12A.

³¹⁰ Peter P Swire and Robert E Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998) 12.

With regard to the second factor, privacy advocates argue that comprehensive legislation will make consumers feel more confident in conducting transactions with businesses through the Internet.³¹¹ Such legislation would grant individuals the knowledge and control of who collects and uses their personal information, when it is collected, and what happens to their personal information after it has been collected and used in the first instance.

The author believes that both sides of arguments are strong and well justified. However, the main research issues remain unresolved in the Jordanian context. What will work for Jordan? Can Jordan rely only on a voluntary self-regulatory sectoral approach similar to the approach adopted by the United States as discussed here in this chapter? Or should it rely on comprehensive legislation as postulated by the privacy advocates?

However, any immediate answer to these issues would be premature. This is because an example of the opposite regime to self regulation has not yet been examined. Therefore, the next chapter provides an examination of one of the most influential approaches to privacy protection, the European Union regime. The intention here is to provide as many details and facts as possible in order to examine whether this alternative approach would better address the issue of privacy in Jordan. However, before reaching to this point, here below is a summary of the current chapter.

³¹¹ Wakana, above n 307, 162.

7.6 Concluding Remarks

This chapter has portrayed a number of features of privacy protection in the US legal system. First, the *US Constitution* does not explicitly express the right to privacy. This has resulted in different interpretations of and meanings for privacy. For instance, despite the US Supreme Court having held that individuals may have an at least limited constitutional right to privacy, these constitutional rights protect individual privacy only against government intrusions, and not private sector intrusions. For example, the *Fourth Amendment* of the *US Constitution* prohibits unreasonable searches and seizures. However, the Court has stated that a privacy right under this amendment has little application outside of the context of the investigation and prosecution of criminal activity. In addition, the *Fourth Amendment* restricts government from interfering with private property, ensures that it must pay compensation for unwarranted government intrusion, provides for due process, and protects citizens from self-incrimination.

Second, the restriction on government actions concerning individual privacy under the *First Amendment* to government legislation and regulations implemented by and for government and governmental agencies has led the US government to rely heavily on the private sector implementing self-regulatory mechanisms for privacy protection within this sector. This reliance has been noted in the FTC report to Congress where it claimed that self-regulation was the ‘most efficient and the least intrusive measure to

ensure fair information practices online’,³¹² including full implementation of measures designed for privacy protection in information and communications technology area.³¹³

The third feature of privacy protection in the US legal system is that the United States views privacy as a property right rather than a human right. Therefore, the US approach to privacy protection is driven by business interests. This feature stems from the philosophy that the United States champions the ‘free flow of information’, and believes privacy laws or data protection laws may damage the national economy.

³¹² Federal Trade Commission, *Self-Regulation and Privacy Online*, Statement before the Subcommittee on Communications (Committee on Commerce, Science and Technology, US Senate (27 July 1999), above n 296, 4.

³¹³ Ibid.

Chapter Eight

The Legal Landscape of Privacy Protection in Europe: The *EU Directive 95/46/EC*

8.1 Introduction

Unlike the United States and Jordan, the European Union adopts a comprehensive approach to privacy protection. The European Parliament has enacted the *EU Data Protection Directive 95/46/EC* (*EU Directive*),¹ which is the most significant piece of legislation providing protection for personal privacy. The aim of this chapter is to compare European law for the protection of privacy with that of the US. It also aims to examine whether or not the *EU Directive* is suitable for use by Jordan as a model law for the protection of individual privacy. There are a number of reasons for examining the EU law. These include:

(1) *The EU's adoption of a comprehensive approach to privacy protection.* The EU law views privacy as part of human rights rather than a type of property rights. This approach is, to a certain extent, similar to the view taken by the *Shari'ah* (Islamic Law), which — as has been noted in Chapter Two — is one of the major sources of Jordanian law. Due to this similarity, any legal reform in Jordan to introduce privacy regulation could logically be influenced by the *EU Directive*, so an examination of its nature and scope is highly desirable.

(2) *The EU's requirement that the transfer of personal information to a third country is permissible only where that third country has a level of privacy protection*

¹ *Directive 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* [1995] OJ L 8/1. See Appendix D.

deemed adequate by the EU for such information. Currently, in the eyes of the EU, Jordan is a place that does not provide adequate protection for personal information. This chapter examines whether or not an agreement similar to that which has at its core the *US-EU Safe Harbour Privacy Principles* could be established between Jordan and the EU to address this matter. The fundamental differences between the US and EU approaches to privacy protection encouraged both regimes (the US and the EU) to close the gap by establishing a *US-EU Safe Harbour Privacy Framework* and adopting the *Safe Harbour Privacy Principles*.² A discussion of these *Principles* is presented in this chapter.

(3) *The existing strong cooperation between the Jordan and the EU (as shown in Chapter Five).* Through the *Association Agreement (AA)*, Jordan and the EU aim to achieve sustainable political, social and economic developments that will affect people's lives positively in Jordan.³ This ongoing commitment to cooperation makes necessary an examination of the EU legislation.

There are a number of issues to be examined in this chapter that concern individual privacy in Jordan. The first issue is whether — based on the *EU Directive* provisions — Jordan is a place that is inadequate in regard to its ability to provide protection to individual personal information; and, in this context, what does constitute 'adequacy'. Secondly, how can Jordan meet the *EU Directive* requirements for personal information protection; and, thirdly,

² US Department of Commerce, 'US-EU Safe Harbour Framework: A Guide to Self-Certification' (2009) available at: <<http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf>>.

³ *EURO-Mediterranean Agreement: establishing an Association between the European Communities and their Member States, of the one part, and the Hashemite Kingdom of Jordan, of the other part*, OJ L129/3, Vol 45, 15 May 2002.

whether or not a compromise agreement on privacy between Jordan and the EU would be sufficient to achieve sufficient privacy protection, rather than requiring Jordan to frame, legislate and implement a 'full EU-style' comprehensive approach to privacy.

The Chapter begins by examining the background to the *EU Directive*. The scope of the Directive is then discussed and reference made to its most significant provisions, namely Articles 25, 26 and 29, which are examined below. The chapter also examines the compromise agreement reached by the EU and US in the *Safe Harbour Privacy Principles*.

8.2 Background to the *EU Data Protection Directive 95/46/EC*

As has been mentioned previously, in the EU privacy is regarded as a fundamental human right. Although this view has 'deep roots in the civil law traditions',⁴ the introduction of privacy or data protection laws by some European countries partly resulted from the horrific memories of the crimes committed during the Holocaust by the Nazi regime of the Third Reich. Such crimes were facilitated by the availability of personal information, which was used to eliminate members of particular racial or other groups of persons.⁵ This shameful experience had taught the European nations the importance of personal information privacy and how such information can be wrongfully

⁴ Barbara Crutchfield George, Patricia Lynch and Susan J Marsnik, 'U.S. Multinational Employers: Navigating through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive' (2001) 38 *American Business Law Journal* 735, 743.

⁵ Approximately 6 million Jews, 2 million Slav civilians, 500,000 Romanians (gypsies) as well as about 500,000 of the mentally ill or incapable, and the physically handicapped, Jehovah's Witnesses (up to 5,000) and others opposed to war, or those viewed as 'unnatural' (homosexual) (circa 10,000); sources various including Amy Monahan, 'Deconstructing Information Walls: The Impact of the European Data Directive on US Businesses' (1998) 29 *Law and Policy in International Business* 275, 283; Israel Gutman (ed), *Encyclopedia of the Holocaust* (Yad Vashem and Macmillan, 1990) 1799; US Holocaust Memorial Museum website <<http://www.ushmm.org/>>.

used for the oppression of innocent civilians.⁶ Most of the European national constitutions have recognised the right to privacy. While the scope of this chapter is limited to an examination of the *EU Directive*, it is worth making a brief reference to European countries that granted a constitutional protection to privacy. For example, in Germany the right to privacy can be extracted from the terms ‘dignity and freedom of personality’ stated in the post-war *German Constitution of 1949*.⁷ In another example, the *Spanish Constitution of 1978*, the right to privacy extends to the protection of personal information stored in electronic devices.⁸ The *Spanish Constitution* provides that ‘the law will limit the use of information in order to safeguard the honour and privacy of the person and the family of citizens and the full exercise of their rights.’⁹ It can be argued that this explicit protection can be extended to include personal information being processed and stored in information and communication technologies. Furthermore, most European countries — including: Austria, Denmark, France, Ireland, Luxembourg, the Netherlands, Sweden, and the United Kingdom — have broad national privacy protection laws governing both public and private sectors concerning the processing of personal information.¹⁰

⁶ Solveig Singleton, *Privacy and Human Rights: Comparing the United States to Europe* (White Paper prepared for the ‘Rights, Rules and Regulations: The Future of Financial Privacy’ Conference of the Competitive Enterprise Institute, Washington DC, 30 November – 1 December 1999) (1999) CATO Institute <<http://www.cato.org/pubs/wtpapers/991201paper.html>> at 8 April 2010.

⁷ David H Flaherty, *Protecting Privacy in Surveillance Societies* (1989) 23.

⁸ Jennifer M Myers, ‘Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States’ (1997) 29 *Case Western Reserve Journal of International Law* 109, 113.

⁹ *Spanish Constitution of 1978*, art 18.4.

¹⁰ Monahan, above n 5, 283.

The recognition of privacy rights by individual European nations led the Organisation for Economic Cooperation and Development (OECD) in 1980¹¹ to adopt international guidelines with regards to information privacy; but, as mentioned in Chapter Two, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)* are in the form of recommendations only and they are non-binding even for countries that have agreed to them. Furthermore, the OECD does not have the power to enforce its guidelines, and it seems unable or unwilling to play a major role in bringing countries to work together to bridge their different standards on the issue of privacy protection.¹²

A number of European countries found the OECD Guidelines unsatisfactory as they failed to provide comprehensive binding legislation for privacy protection. In 1981, the Council of Europe (CE), an organisation of 47 countries that aims to 'protect human rights, as well as strengthen democracy and the rule of law',¹³ issued a set of principles in the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (the Convention).¹⁴ The goal of such principles is to create uniform, binding legislation on data protection. However, the Council failed to achieve this goal because it could not force its members to implement the principles

¹¹ Organisation for Economic Co-Operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) OECD <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html> at 10 April 2010.

¹² Julia M Frombolz, 'The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 461, 467.

¹³ Council of Europe, *Council of Europe in Brief: Mission Objectives* CE <<http://www.coe.int/aboutcoe/index.asp?page=nosObjectifs&l=en>> at 9 April 2010.

¹⁴ Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981) Council of Europe <<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>> at 9 April 2010.

of the Convention in their national legislation. Additionally, the Convention failed to define key terms in the context of data protection.¹⁵ Neither do the OECD Guidelines nor the principles of the 1981 European Convention provide specific privacy protection for personal information. However, both documents agreed to certain common principles, namely the need for law on privacy protection, the encouragement of the flow of information among Member states, and the need for restrictions on the transfer of information to countries which do not have adequate privacy protection.¹⁶ Based on these common principles, the *EU Data Protection Directive 95/46/EC of 1995* was created.

8.3 The Scope of the *EU Data Protection Directive 95/46/EC*

The *EU Directive 95/46/EC* on the ‘Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data’ entered into force on 24 October 1998. The Directive has cited Article 8 of the *European Convention on Human Rights* which sees privacy (as previously discussed in Chapter Two) as a fundamental human right. The citation of Article 8 in the *EU Directive* gives a strong indication that the Directive is very concerned to provide the ultimate protection to the right of privacy.¹⁷ Further, the Directive’s object is to protect privacy that is part of the

¹⁵ Frombolz, above n 12, 467.

¹⁶ George, Lynch and Marsnik, above n 4, 745.

¹⁷ *Directive 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* [1995] OJ L 8/1 Recital 10 (the *EU Personal Data Privacy Directive*) (citing Article 8 of the *European Convention on Human Rights*): ‘Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community’.

fundamental rights and freedoms of natural persons.¹⁸ The Directive seeks to encourage the free flow of personal information between Member States while protecting this fundamental right.¹⁹

As a starting point, the Directive contains a number of significant regulatory provisions in relation to the processing of personal information or data. The Directive defines 'personal data' as 'any information relating to an identified or identifiable natural person'. An identified or identifiable person is defined by the Directive as 'a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological mental, economic, cultural or social identity'.²⁰ The scope of this definition extends to the 'processing'²¹ of personal information 'wholly or partly' by electronic means, and to the processing of personal information that is part of a 'filing system'²² or will become part of a filing system.

It appears from the above definition that European businesses can collect, process, disclose, use and share information about individuals only when this

¹⁸ Ibid art 1(1) states: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedom of natural persons and in particular their right to privacy with respect to the processing of personal data'.

¹⁹ Ibid art 1(2) states that: 'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1'.

²⁰ Ibid art 2(a).

²¹ Ibid art 2(b) defines 'processing' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organising, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure of destruction.'

²² Ibid art 2(c) defines 'filing system' as 'any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis'.

information cannot be linked with a particular person.²³ The transfer of personal information so linked between Member States or the collection of such information across national boundaries (that is by an organisation in one country from persons in another) would contravene Article 1 of the Directive.

The processing of personal information included in the above definition is not subject to the Directive's protection in two situations. First, the Directive is not applicable to activities which require the processing of information in regard to public security, defence, State security and the activities of the State in areas of criminal law.²⁴ This situation reflects the objective of the Directive, namely that it intends to regulate the activities carried out in the private sector rather than the public sector.²⁵

Secondly, the demands of the Directive can be ignored where the processing of personal information is conducted by 'a natural person in the course of a purely personal or household activity'.²⁶ This exemption may allow a person or household to process a number of pieces of personal information for personal use without the need to comply with the Directive. For example, a person based in a Member state can keep contact information lists and send such a list out for family purposes. The processing of such information will not be protected by the Directive's provisions. However, this situation may

²³ Steven R Salbu, 'The European Union Data Privacy Directive and International Relations' (2002) 35 *Vanderbilt Journal of Transnational Law* 655, 670.

²⁴ *EU Personal Data Privacy Directive* [1995] OJ L 8/1, art 2.

²⁵ Peter P Swire and Robert E Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998) 27.

²⁶ *EU Personal Data Privacy Directive* [1995] OJ L 8/1, Ibid art 3(2).

cause confusion when reading the terms of Article 3(1).²⁷ Does personal information — which may include personal and business names and contact details, stored in someone’s personal database (personal computer) — fall within the scope of Article 3(1), and therefore, require the Directive protection?²⁸

The Directive also imposes obligations on the controllers (defined by the Directive as ‘any person who determines the purposes and means of the processing of personal data’) and the processors (defined as ‘any person [who] processes personal data on behalf of the controller’) of personal information. The Directive also provides set rights that are available to persons who are the data subjects.²⁹

The Directive requires that controllers and processors of personal information must ensure that the information is collected and processed for legitimate, specific purposes, and that it is accurate and kept in a form which permits identification of the data subject for no longer than is necessary to achieve the legitimate purposes for which the information was originally collected and processed.³⁰

Furthermore, the Directive requires that persons (data subjects) are to be given information related to the identity of the controller, the purposes of the

²⁷ Ibid art 3(1) provides that ‘This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system’.

²⁸ Swire and Litan, above n 25, 27.

²⁹ *EU Personal Data Privacy Directive* [1995] OJ L 8/1, art 2(d)(e).

³⁰ Ibid art 6.

collection, and any other information relevant to them (the data subjects).³¹ Additionally, the Directive grants persons the right to access and correct information that has been collected about them.³²

More importantly, in order to protect the subjects' personal information, the Directive provides individuals with the right to 'opt in' rather than 'opt out' in relation to the provision of personal information and its subsequent processing. According to the 'opt-in rule', personal information may be processed only if an individual has unambiguously given their consent.³³ This rule requires that individuals should be asked for their assent to the collection and to processing of their personal information prior to its collection (and processing, and its extent, including its use, disclosure, sharing and transfer). The opt-in rule allows individuals to say 'yes' or 'I approve', or 'I accept' the processing of 'my personal information'. Indeed it makes such a question/approval process mandatory.

In contrast, the 'opt-out' rule imposes the burden of preventing the processing of personal information on the individuals supplying the information. The opportunity to assent is omitted. In the case of the opt-out rule, unlimited collection of personal information is allowed unless the individual concerned says 'stop' or simply ceases to supply the requested data. The opt-out rule has been favoured by the United States (as discussed in the previous chapter). The Directive, on the other hand, requires further

³¹ Ibid art 10.

³² Ibid art 12.

³³ Ibid art 7(a).

restrictions on specific areas of information, in addition to compliance with the opt-in rule. This information includes revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or criminal convictions, or information concerning a person's health or sex life.³⁴

The *EU Directive* also provides individuals with the explicit right to object to any processing of their personal information for commercial purposes, and with the right to be informed before their personal information is disclosed for the first time to third parties for commercial purposes. Individuals should be able to exercise this right (the right to object) free of charge upon their request.³⁵

With respect to the remedies, the Directive grants individuals a personal right to judicial remedy when an individual's information is being processed contrary to its provisions.³⁶ Further, the Directive requires that Member states both provide individuals with compensation for damages suffered, and impose sanctions on the controller if the controller is found to be liable for an act that caused the damage.³⁷

Finally, the most significant provisions of the Directive are those contained in Articles 25 and 26, the main concerns of which are focused on the transfer of information to third countries. They have a noticeable impact on countries

³⁴ Ibid art 8(1).

³⁵ Ibid art 14.

³⁶ Ibid art 22.

³⁷ Ibid art 23.

outside the zone of the European Union, such as the United States and, eventually, Jordan. The European Union has determined that:

[The] United States does not provide adequate privacy protection, as the United States lacks to any applicable legal data protection in the private sector and virtually all data are processed without specific guarantees of judicial protection.³⁸

To address the issue of privacy protection ‘adequacy’, the US and the EU adopted in July 2000 an agreement which involves what are known as the *Safe Harbour Privacy Principles*. US companies that agree to comply with these are allowed to transfer information beyond the EU jurisdiction. The *Safe Harbour Privacy Principles* are discussed below.

In the eyes of the EU Parliament, Jordan is also considered as a place that does not provide adequate privacy protection. There are no specific legal principles applicable to data protection in Jordan, either for the public or the private sector. The inadequacy of the Jordanian law concerning privacy may therefore prevent the flow of personal information between the EU and Jordan, with serious implications for free trade, economic growth, and the operation of businesses that rely on the flow of information.³⁹ The following sections examine the adequacy requirement included in the *EU Directive* and its effects on Jordan.

³⁸ European Parliament, 'Report on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles (C5-0280/2000-2000/2144 (COS)' (RR\285929EN.doc, 2000), 7-8, avail at: <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/0117-02_en.pdf>.

³⁹ David A Tallman, 'Financial Institution and the Safe Harbor Agreement: Securing Cross-Border Financial Data Flows' (2003) 34 *Law and Policy in International Business* 747 754.

8.3.1 Article 25 and the requirement for ‘adequacy’

Article 25(1) of the *EU Directive* governs the transfer of personal information outside the jurisdictions of the EU Member States. This Article states that:⁴⁰

The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection.

The main element of the above Article is that third countries receiving information from the EU Member States must ensure an adequate level of privacy protection. The adequacy of a country’s privacy protection is decided on a number of specific elements: (a) ‘the nature of the data’, (b) ‘the purpose and duration of the proposed processing operation’, (c) ‘the country of origin and the country of final destination’, (d) ‘the rules of law, both general and sectoral, in force in the third country’, and (e) ‘the professional rules and security measures’ that are implemented in the third country.⁴¹

Based on the above elements, the following example, supported by Figure 6 (below) is used to illustrate whether or not adequate privacy protection is afforded in Jordan as a third country. For example,

France Telecom owns 51 per cent of the Jordan Telecommunication Company (JTC) (located in Jordan-Amman) which has 1.613 million mobile customers, 506,000 fixed-line customers and 119,000 Internet users as at June 2009.

⁴⁰ *EU Personal Data Privacy Directive* [1995] OJ L 8/1, art 25(1).

⁴¹ *Ibid* art 25(2).

Assume that France Telecom requires all personal information (data) about JTC customers to be processed by the main company (France Telecom) which is located in France.

Assume further that a marketing company, ABC, is an affiliate of France Telecom and wishes to use the personal information accumulated by France Telecom about the JTC customers for marketing purposes. Part of ABC's marketing activities is to send personal information to other affiliated companies based in Jordan.

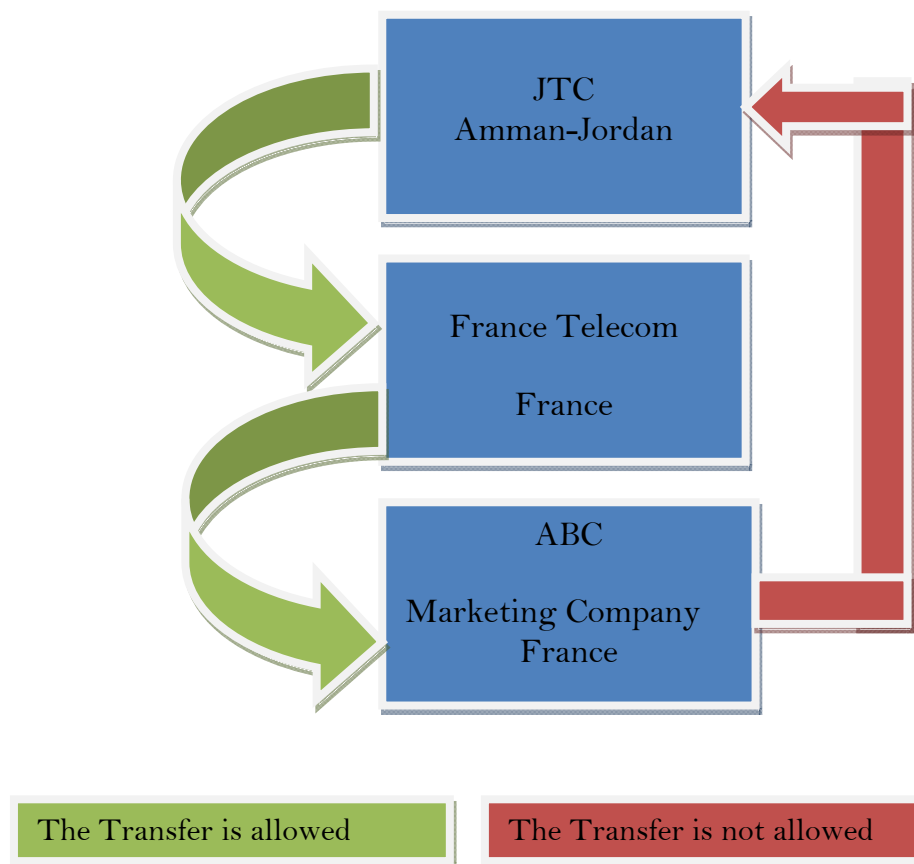
The important issue illustrated by the above example is that the transfer of personal information from JTC in Jordan to its parent company (France Telecom) in France is an activity that current Jordanian law would allow. This is simply because there are no particular laws or regulations that would prevent or govern such transfers. Furthermore, both France Telecom and ABC would be able to process personal information received from JTC as both companies are subject to the *EU Directive 94/46/EC*. In contrast, neither ABC nor any other company in France would be allowed to send personal information about JTC customers to its affiliates in Jordan. The lack of both specific legal principles and security measures for privacy protection as required by Article 25 of the *EU Directive* in the third party country will prevent such transfer to Jordan as a third country as the those involved in the treatment of data in Jordan are not currently required to observe the same high standards of privacy protection.

The below figure clearly shows the imbalance of the relationship regarding information flow between the two countries. Article 25 of the *EU Directive*

would ‘threaten to impose an embargo on personal information data flows’⁴² to Jordan as Jordan does not meet the required standard of adequacy. In contrast, personal information is moving freely from Jordan to the EU zone without any restrictions. This imbalance in the relationship between the EU and Jordan may only benefit businesses based in the EU jurisdiction rather than businesses based in Jordan.

Figure 6

The Flow of Personal Information Cycle between Jordan and the EU Member States



8.3.2 Article 26 and exemption from the ‘adequacy’ requirement

Under the *EU Directive*, a person may transfer personal information to third countries even when that country does not provide an adequate level of

⁴² George, Lynch and Marsnik, above n 4, 737.

privacy protection. Article 26 of the Directive provides six exceptions to the prohibition under Article 25. These exceptions may apply in the following situations: (a) ‘the data subject has given his consent unambiguously to the proposed transfer’, (b) ‘the transfer is necessary to perform a contract between the data subject and the controller’, (c) ‘the transfer is necessary for the performance of a contract concluded in the interest of the data subject’, (d) ‘the transfer is necessary on important public interest grounds’, (e) ‘the transfer is necessary in order to protect the vital interests of the data subject’, and (f) ‘the transfer is made from a register which according to laws or regulations is intended to provide information to the public’.⁴³

With respect to the first exception that a person’s unambiguous consent must be obtained before the transfer of his/her personal information, it is further required that any consent to transfer personal information is only applicable to the particular uses of his/her personal information where notice has been given to the this person (the data subject).⁴⁴

The second exception permits the transfer of information in order to complete a contract between the data subject and the controller. For example, an individual in Europe wishes to purchase an item from a Jordanian merchant. In order to complete the purchase, the seller requires the buyer’s name and address. However, the seller may also seek additional information about the buyer such as: annual income, marital status, age and other information, for the purpose of completing the transaction. The issue

⁴³ *EU Personal Data Privacy Directive* [1995] OJ L 8/1, art 26.

⁴⁴ Swire and Litan, above n 25, 34.

here is whether this additional information is necessary to complete the contract and, therefore, permit the transfer of buyer's personal information. If the information requested by the seller is actually unnecessary to complete the transaction, the seller may need to obtain unambiguous consent from the buyer to acquire such additional information.⁴⁵

With regard to the third exception, this Article permits the transfer of personal information between the controller and a third party in the interest of the data subject. For example, a resident in Europe wants to send money to his family in Jordan. In order to complete this transaction, the European resident must give his name and account number to his local bank, and, in turn, the bank passes this personal information to another bank (the third party). This transfer of personal information to a third party is permitted because it is necessary to complete the transaction which is being concluded in the interest of the European resident.⁴⁶

The fourth exception is based on 'important public interest grounds'. This exception appears to apply to important public issues as defined by either Europe or third countries. For example, this exception may be applied to the so-called 'war on terror' where personal information can be transferred between Europe and Jordan for public interest (security) purposes.

The fifth exception addresses similar issues. Transfer of personal information is permitted in order to 'protect the vital interest of the data subject'. This could occur, for example, in a medical emergency where the transfer of a

⁴⁵ Ibid 34.

⁴⁶ Ibid 35.

patient's information to third parties in a foreign country may be vitally necessary at the time when the patient is unable to give unambiguous consent.⁴⁷

Lastly, personal information can be transferred to third countries when the transfer is made from a register 'intended to provide information to the public'. For instance, personal information can be sent to the public in Jordan in order to receive general feedback on the trade agreements between Jordan and the EU. Therefore, the transfer must be to the public or to a person who can demonstrate legitimate interest, in accordance with laws or regulations.⁴⁸

8.3.3 Article 29 and the 'Working Party'

Article 29 plays as a mechanism in determining whether a country -or Jordan as stated in the above example- has an adequate privacy protection or not. Article 29 of the Directive called for the establishment of a 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' ('Working Party').⁴⁹ Article 29 grants the Working Party advisory status and the ability to act independently.⁵⁰ It is composed of a representative of the supervisory authorities for each Member state and a representative of the European Commission.⁵¹ Decisions are taken by the Working Party by a

⁴⁷ Ibid 36.

⁴⁸ *EU Personal Data Privacy Directive* [1995] OJ L 8/1, art 26(1)(f).

⁴⁹ Ibid art 29.

⁵⁰ Ibid art 29(1).

⁵¹ Ibid art 29(2).

simple majority of the representatives of the supervisory authorities.⁵² The Working Party is to elect a chair for two years.⁵³

The Working Party plays an important role in determining what constitutes 'adequate protection'. Although the Working Party has no explicit role in making decisions about particular cases, in general the group's work can provide guidance on how to evaluate adequacy. Further, because it has an advisory status, the Working Party can advise the Commission on various issues with respect to any transfers of information to third countries on a 'case by case' basis.⁵⁴

The Working Party's views on adequacy are influential because, under the Directive, each Member state's supervisory authority selects a representative to serve as a member of the Working Party. In addition, these representatives are experts in the field of privacy protection. Any advice presented by them to the Commission may be recognised as future policies in the context of privacy protection.⁵⁵

On the issue of 'adequacy', the Working Party has presented some explanations on the issue of 'adequate' protection as a requirement under Article 25 in relation to allowing the transfer of personal information to third countries. The Working Party has commented on this issue by stating that:

For its part, the Committee regards it as necessary to be even-handed in implementing the provisions of the Directive that deal with third countries.

⁵² Ibid art 29(3).

⁵³ Ibid art 29(4).

⁵⁴ Patrick J Murray, 'The Adequacy Standard Under Directive 95/46/EC: Does US Data Protection Meet this Standard?' (1998) 21 *Fordham International Law Journal* 932, 999.

⁵⁵ Ibid.

The Committee expresses its commitment to the principle of non-discrimination and recalls that the general principle of equality, of which the prohibition of discrimination in grounds of nationality is a specific enunciation, is one of the fundamental principles of Community law. This principle requires that similar situations shall not be treated differently unless differentiation is objectively justified. The Committee also recalls obligations emanating from other international instruments, in particular the European Convention of Human Rights. Article 14 of the ECHR requires that the rights and freedoms set forth in the Convention (which include the right to respect for privacy - Article 8) be secured without discrimination on any ground, including *inter alia* national origin.⁵⁶

This is not to mean that all countries are expected to adopt identical provisions for privacy protection but rather that overall effectiveness must be maintained. The Committee notes that it

regards it as important to be able to judge different situations on their merits and not to regard the equal treatment principle as imposing a single model on third countries. Such an interpretation of the principle would fly in the face of the deliberately flexible wording of Article 25 (which requires “adequate” protection in third countries and which allows circumstances to be judged on a case by case basis) and of the need to take into account different countries’ varied approaches to achieving effective data protection. This approach means that adequacy findings may sometimes be made despite certain weaknesses in a particular system, provided of course that such a system can be assessed as adequate overall, for example because of compensating strengths in other areas. The principle of equal treatment does not mean that allowances made to take account of the particular traditions of one country, as described above, are automatically applicable to or acceptable in the cases of other third countries. It does mean that assessments of adequacy should be made broadly by reference to the same standard...⁵⁷

However, the Working Party claimed that in order for protection to be considered adequate, any data protection policy is required to have ‘content’

⁵⁶ *Text on Non-Discrimination Adopted by the Article 31 Committee on May 31, 2000* <<http://www.ita.doc.gov/td/ecom/nondiscrimArt31May00.htm>> at 16 June 2010.

⁵⁷ *Ibid.*

principles and ‘procedural/enforcement’ as minimum requirements. Regarding the content principles, a number of basic principles are to be included: (1) the ‘purpose limitation’ principle, (2) the ‘data quality and proportionality’ principle, (3) the ‘transparency’ principle, (4) the ‘security’ principle, (5) the ‘right to access, rectification and opposition’, and (6) restrictions on ‘onward transfers’.⁵⁸ It is worth mentioning that these principles are similar to those included in the OECD guidelines of 1981.

With respect to ‘enforcement’ mechanisms, the Working Party believed that in order to provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries. For this matter, the objectives of a data protection system aim to: (1) ‘provide a good level of compliance’, (2) provide ‘support and assistance to individual data subject to exercise their rights’, and (3) ensure ‘appropriate redress’ to the injured party where rules have been violated.⁵⁹

In sum, it is important to point out that the Directive is a major achievement in relation to the protection of personal information, not for just Europe but for the entire world. It ‘represents the most modern international consensus

⁵⁸ European Commission, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (1998) <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf> at 16 June 2010.

⁵⁹ Ibid.

on the desirable content of data protection rights and may be a valuable model for countries without data protection laws'.⁶⁰

However, the Directive has a number of weaknesses that may undermine its application. First, it is incongruous to require equivalent protection in the Member States and merely 'adequate' protection for transfer to a third country. Logically, individuals are likely to be unaware of how their personal information is to be treated in third countries. As a result, transfer to such third countries must be recognised as inherently of greater risk than the use of information within the Member States.⁶¹

A second weakness of the Directive is located in Article 26(2) which permits the use of a contract as an exception to the adequacy requirement. This exception provides a 'contractual solution' to the challenge of inadequate privacy protection. This solution, however, raises a concern for whether a contract — rather than comprehensive legislation — can provide the desired protection to personal information.⁶² Further, the use of a contract means that the data subject is not a party to the contract and has no direct control over its terms and provisions.⁶³ For instance, a company based in Jordan can enter into a contract with a European company on sharing information about their clients. However, both legal systems will have different interpretations as to any rights or obligations imposed on the clients. When disputes arise,

⁶⁰ Graham Greenleaf, 'The 1995 EU Data Protection Directive on Data Protection: An Overview' (1995) 3(2) *International Privacy Bulletin* 1

⁶¹ Paul M Schwartz, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 *Iowa Law Review* 471, 485.

⁶² *Ibid* 486.

⁶³ Alison White, 'Control of Transborder Data Flow: Reactions to the European Data Protection Directive' (1997) 5(2) *International Journal of Law and Information Technology* 230, 241.

the clients in Jordan will face great difficulty in taking action against any violations committed by the other company which based in Europe. Further, the client whose personal information has been shared will not have the right to express any objections to the transfer of information between the two companies.

Thirdly, Articles 25 and 26 of the Directive create difficulties for international businesses, and particularly for businesses which mostly rely on the transfer of personal information to conduct their businesses (such as: credit reporting agencies, banks, hotels and airline booking systems, and life insurance firms).⁶⁴ At the time of writing, there are no available reports or statements issued by the European Union to indicate that Jordan provides an 'adequate' level of privacy protection, that is, one that meets EU standards. Categorising Jordan as a non-compliant country in terms of the *EU Directive* requirements may disadvantage Jordanian companies who would like to benefit from the trade agreements signed with EU, and render useless the privatisation process implemented by Jordan, and, as a result, set back the country's economic growth.

The main question, here, is how Jordan's companies can meet the Directive's 'adequacy' requirement in order to earn access to the European information? Can Jordan and the EU arrange for a special agreement similar to that embodied in the *US-EU Safe Harbour Privacy Principles*? The following sections examine, first, the basis for the 'Safe Harbour' agreement, and its

⁶⁴ Colin J Bennett and Charles D Raab, 'The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response' (1997) 13 *The Information Society* 245, 254.

critics. Discussion then continues to examine the suitability of a similar 'Safe Harbour' agreement for Jordan and the EU in order to meet the Directive requirements. It may conclude that Jordan needs to enact its own privacy protection law rather than an agreement to receive EU recognition.

8.4 The US-E.U Safe Harbour Privacy Principles

8.4.1 Background

The strong requirements for privacy protection included in the EU Directive have categorised the US regime as being an inadequate regime for privacy protection. This was due to the lack of a comprehensive approach to privacy protection in the United States. The impact of this categorisation was felt by US companies that rely on transactions involving personal information of EU citizens. In order to address the question of what measures should be implemented to close the gap between the US and EU regimes, the US Department of Commerce (DOC) and an EU working party started two years of negotiations that have resulted in July 2001 the announcement of the *Safe Harbour Principles*.

The *Safe Harbour Privacy Principles* provides voluntary participation, self-regulation and a privacy policy framework for US companies. If US companies choose to participate, they must comply with the requirements of the *Safe Harbour Privacy Principles* and publicly announce that they do so.⁶⁵ US companies must further self certify annually to the DOC in writing that they agree to fully comply with the principles and requirements included in

⁶⁵ US Department of Commerce, *EU Safe Harbour Overview* US DOC <http://www.export.gov/safeharbor/eu/eg_main_018476.asp> at 9 June 2010.

the *Safe Harbour Privacy Principles*.⁶⁶ However, companies that violate these requirements and principles after joining the *Safe Harbour Privacy Principles* agreement may be subject to prosecution in accordance with US laws dealing with fraud and misrepresentation, such as the *False Statements Act* (18 USC 1001).⁶⁷ Any discussions on such laws are beyond the scope of this research.

The DOC has summarised the benefits of joining the *Safe Harbour Privacy Principles* agreement. First, the US companies participating will be recognised by all EU Member states as legitimate businesses able to deal with the personal information of EU citizens. Secondly, approval of data transfers from Europe to participating companies will be waived or automatically granted; and, finally, any claims against participating US companies by EU citizens will be heard before the US court and will be subject to the US law.⁶⁸ Such guarantees have made the *Safe Harbour Principles* more attractive to US companies than might otherwise have been the case. Approximately 3,000 companies are enrolled in Safe Harbour. Of these, about 20% are listed as not current.⁶⁹

8.4.2 The Safe Harbour Principles

For a company to receive the above benefits, it must incorporate and address the *Safe Harbour Principles* in its privacy policy. The principles consist of seven requirements which are identical of those of the *EU Directive*. These principles are:

⁶⁶ Ibid.

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹US Department of Commerce, *Safe Harbor List*, avail: <http://safeharbor.export.gov/list.aspx> at 8 June 2011.

1. Notice: the company must inform individuals about the purposes for which it collects and uses information about them, how to contact the company with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the company offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the company or as soon thereafter as is practicable, but in any event before the company uses such information for a purpose other than that for which it was originally collected or processed by the transferring company or discloses it for the first time to a third party.

2. Choice: the company must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorised by the individual.

3. Onward Transfer: Third parties receiving the information are required by the company to provide the same level of privacy protection as the company itself.

4. Security: companies must secure the data and prevent the loss, misuse, disclosure, alteration, and unauthorised access of personal data.

5. Data Integrity: A company may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorised by the individual. Individuals must be reassured that their data is complete, accurate, current, and used for its intended purpose only.

6. Access: individuals must have access to personal information about them that company holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case of question, or where the rights of persons other than the individual would be violated.

7. Enforcement: effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the company when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up

procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by companies announcing their adherence to them and consequences for such companies.⁷⁰

The DOC and the European Commission praised the above Principles as a successful program. The Principles are seen as consistent and affordable channels permitting third countries to continue transferring personal information outside the EU.⁷¹ However, the *Safe Harbour Principles* have been criticised by a number of privacy advocates. With respect to the principle of 'Choice', the right to 'opt out' is insufficient because it requires individuals to check an 'opt out' box every time they enter a transaction. It is recommended that individuals have the right to 'opt in' so that personal information may not be used or transferred unless an explicit consent obtained from individuals.⁷² (The 'opt out' and 'opt in' rights were earlier discussed).

With regard to the principle of 'Access', privacy advocates have suggested that an individual's right must extend to all type of information collected about them, not just 'sensitive' information (which has not been defined by the *Safe Harbour Privacy Principles*).⁷³ One important criticism outlined by privacy advocates is the lack of adequate enforcement mechanisms. For example, a participating US Company may violate any *Safe Harbour Principles* that would lead to thousands of instances of stolen identity, yet under the

⁷⁰ US Department of Commerce, 'US-EU Safe Harbour Framework: A Guide to Self-Certification' (2009) 12–14, available at: <<http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf>>.

⁷¹ Mark S Merkow and James Breithaupt, *The E-Privacy Imperative: Protect Your Customers' Internet Privacy and Ensure Your Company's Survival in the Electronic Age* (2002) 82.

⁷² Gregory Shaffer, 'Globalisation and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards' (2000) 25 *Yale Journal International Law* 1, 64.

⁷³ *Ibid* 65.

Safe Harbour Privacy Principles, the company has no requirement to inform EU citizens affected. The EU citizens would then be forced to become 'police agents' and report the Safe Harbour violations on their own accord, but it would be impossible for them to identify the company that was the source of the data breach.⁷⁴

Furthermore, some believe that the *Safe Harbour Privacy Principles* may not successfully achieve the goals included in the US-EU negotiations. The purpose of these negotiations is to ensure a smooth flow of information between US and EU. At the same time, US businesses are required to provide adequate protection for information received from the EU citizens. The 'Safe Harbour' may not succeed in attaining these goals due to one significant reason: the way in which the United States addresses the issue of privacy is fundamentally different to the way in which it is addressed by the EU. The EU encourages the use of government power to enforce its laws to protect citizens' rights, while the United States expresses its reluctance to impose restrictions on the data flow as it may disadvantage businesses.⁷⁵

Further, the EU has preferred to deal with the central governments of EU Member States while the United States has been reluctant to implement an official government role for the central government.⁷⁶ Despite the DOC having negotiated the *Safe Harbour Privacy Principles Agreement*; it has assigned the private sector to carry out the enforcement of the Agreement,

⁷⁴ Daniel R Leathers, 'Giving Bite to the EU-U.S. Data Privacy Safe Harbour: Model Solutions for Effective Enforcement' (2009) 41 *Case Western Reserve Journal of International Law* 193, 195.

⁷⁵ Priscilla M Regan, 'Safe Harbours or Free Frontiers? Privacy and Transborder Data Flows' (2003) 59(2) *Journal of Social Issues* 263, 274.

⁷⁶ *Ibid* 275.

with some support from government agencies regarding enforcement when there are contraventions of legislation related to ‘unfair and deceptive practices’.⁷⁷ Participant companies must ensure, by following up certain procedures, that their privacy practices are true and have been implemented as presented. In addition, participants companies must meet their obligations to compensate parties in case there is a failure to comply with the Principles.⁷⁸

8.4.3 The Proposal for a Jordan-EU ‘Safe Harbour’ agreement

The *Safe Harbour Principles* are still an important vehicle, setting out basic guidelines for privacy policy at an international level because (as discussed above) they reflect different regimes to privacy protection between two important jurisdictions: the United States and the EU. The main issue, however, is whether or not a similar agreement can be reached between Jordan and the EU in order to meet the *EU Directive’s* ‘adequacy’ requirement.

Further to the above criticisms of the *US-EU Safe Harbour Privacy Principles* agreement, the author believes that while proposing any sort of agreement between Jordan and the EU concerning the flow of personal information may assist in bringing the issue of individual privacy to the fore, it may not actually achieve the most desirable goal, which is to protect individual

⁷⁷ U.S. Department of Commerce, *Safe Harbor Overview* U.S. Department of Commerce <http://www.export.gov/safeharbor/eg_main_018236.asp> at 17 June 2010.

⁷⁸ US Department of Commerce, 'US-EU Safe Harbour Framework: A Guide to Self-Certification' (2009)14, available at: <<http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf>>.

personal information in Jordan and abroad. This belief is based on two factors:

First: The effectiveness of any proposed agreement between Jordan and the EU must be based on a solid legal foundation in order to support and strengthen the proposed bilateral agreement. Currently, Jordan does not have a solid domestic foundation for privacy protection, neither in a form of privacy principles nor in a form of national privacy law.

In contrast, both parties in the *US-EU Safe Harbour Privacy Principles agreement* had some sort of existing privacy principles in their legal system prior to negotiations. As discussed in the previous Chapter, the US legal system has a number of privacy laws that have been enacted to address privacy issues in public and private sectors. As discussed in the previous Chapter, the US legal system is stronger regime than Jordan. It has a number of privacy laws that have been enacted to address privacy issues in public and private sectors. In Jordan, however, there are no specific laws to address privacy issues that arising within certain sectors.

Second: It is believed that achieving a desirable approach to privacy protection in Jordan requires more than a voluntarily agreement. If Jordan and the EU negotiated a similar agreement to the *US-EU Safe Harbour Privacy Principles*, it would not qualify Jordan as a country that provides 'adequate' protection for personal information. Such an agreement might also only be applicable to specific areas of business that voluntarily agreed to participate in the proposed agreement. This means that non-participants

would not have to comply with the principles espoused by the agreement, leaving personal information processed by non-participating businesses outside the scope of the agreement.

8.5 Concluding Remarks

The *EU Directive 95/46/EC* plays a significant role in protecting individual privacy at international level. For Jordan — as a third party — the EU is an important partner. Through the AA (discussed in Chapter Five), both parties are aiming to create a free trade zone by year 2014, on condition that Jordan carry out a number of economic, social and political reforms. On the issue of privacy protection reform, Jordan is yet to meet the requirements of the *EU Directive*.

Under the *EU Directive* provisions that examine the adequacy of a third country's privacy protection, Jordan — as a third country — will not be listed as an adequate recipient of personal information from the EU Member States. This is primarily due to a lack of Jordanian legislation that addresses the treatment of personal information in the public and the private sectors. For instance, privacy protection in the public sector is inadequate, as the case study on privacy and e-government in Chapter Four demonstrated when it was determined that the majority of government agencies in Jordan do not have privacy policies or statements with respect to handling personal information.

Further, under the EU Directive, the private sector in Jordan will also be as 'inadequate' as it fails to provide a minimum of privacy protection. Member

States will, therefore, prevent the transfer any type of information to businesses in Jordan. For instance, as illustrated by the case study in Chapter Five, there is no privacy protection law or guidelines in the area of banking and/or telecommunications industries. Thus, these two specific business areas, like many other business areas and individual businesses in the private sector, do not provide a minimum level of privacy protection for the processing of personal information.

The issue of 'inadequacy' of privacy protection in Jordan leads to the presentation (in the following Chapter) of what could be the most suitable and appropriate approach to privacy protection in Jordan. It proposes a national privacy policy reform that would allow Jordan to be considered as a country with 'adequate' privacy protections in place, and therefore an 'adequate' place for the handling of personal information, not just at the level of private sector, but also at the public sector level.

Chapter Nine

Findings and a Final Thought

9.1 Introduction

In the last decade, Jordan has witnessed significant developments in its economy. The liberalisation of its market, the signing of international trade agreements and the implementation of the privatisation process are the most noticeable changes in Jordan's modern history. One important sector has been chosen to be the subject of this study — the Information and Communications Technology (ICT) sector. Often seen as a success story, it is one of the fastest growing sectors in the country, and its importance cannot be ignored as it affects all aspects of Jordanian society, including telecommunications, education, banking, commerce, and employment. However, the use of information and communication technologies by the public and the private sectors threatens individual privacy and has raised the subject of its protection.

The main question addressed in this thesis is: 'What is the best approach for privacy protection within the Jordanian context?' This is explored in the context of the two main approaches adopted across the world: the self-regulatory approach (as exemplified by the United States) and the more comprehensive and some would say rigorous approach legislative 'rights based' approach (exemplified by the EU). This necessarily involves an exploration of the impact of the differing concepts of the very nature of privacy.

The subject is teased out by a number of subsidiary questions, namely:

1. 'Do individuals in Jordan have the right to privacy?' Associated with this question is whether (and to what extent) this right is guaranteed by the Constitution, international treaties and/or by traditions and beliefs?'
2. 'Do individuals in Jordan need specific legislation to protect their privacy in the ICT sector or, can Jordan rely only on market mechanisms such as self-regulation, technology or government guidelines for protecting privacy?'
3. 'Is self-regulation the most appropriate approach for Jordan?'
4. 'What alternatives may be suitable for the Jordanian legal system to protect privacy?'

The thesis seeks to achieve a number of objectives. It seeks to:

- (a) Formulate a working definition of the concept of privacy.
- (b) Examine the historical principles of privacy in Islam and link these to the modern definition.
- (c) Investigate the position on privacy protection of both the public and private sector in Jordan, using an empirical methodology. This involved an online survey of government websites and the websites of two major areas of the private sector: banking and telecommunications industry
- (d) Identify privacy concerns and threats to individuals in the private sector.
- (e) Critically review and analyse the current legal landscape in Jordan as regards privacy
- (f) Describe and evaluate the self-regulatory approach adopted by the US
- (g) Describe and evaluate the legislative based approach of the EU
- (h) Explore potential options for Jordan.

9.2 Summary of Findings

Chapter 1 – General Introduction. A survey of the literature revealed that although the definition of the concept of privacy is ill-defined, it is nevertheless a generally well-understood concept involving various spheres of privacy (for example, the home, intimate communications between family members, family life); however, that is not to say that there are no cultural variations. For a number of countries (including Jordan), the concept extends to include honour and reputation as important collective familial (and in the case of the reputation of the Prophet (pbuh)) societal values. This view has implications for freedom of expression, which is not held to be of equal value.

Some recent legislation is also seen as potentially invasive of personal privacy, though justified by the government on the basis of security. Apart from the compulsory collection of user data at internet access points, random government surveillance of telecommunications (an activity requiring no warrant nor any suspicion of wrong-doing) has raised concerns, as has the privatisation of formerly government entities and the transfer from government to private hands of vast quantities of data, the security of which, at least in the ICT industry, is unlikely to be able to be guaranteed in the absence of specific legislation to protect privacy. The problem of what is guaranteed by law and what happens ‘on the ground’ is raised — especially given that Jordan is a signatory to a number of international conventions which, in themselves, would seem to guarantee a degree of recognition of the right for privacy (for example, the non-binding 1948 Universal Declaration of Human Rights, Article 12; the binding International Covenant on Civil

and Political Rights, Article 17 and the International Covenant on Economic, Social and Cultural Rights); and while Islam strongly defends individual privacy, law in Jordan remain insufficient to protect this right in terms of both public and private entities.

Chapter 2 – The Concept of Privacy. In a culture where privacy is so highly valued, legislation may be necessary to define the boundaries between the private and public good, where a clash may arise between the public good (for example, in relation to security, transparency of transactions in business) and a right to privacy of person in their communications, banking or other actions. The high level of dependency people have on the Government is a ‘two-edged sword’. On the one hand, people’s reliance on the government to regulate the environment can be seen as favouring the introduction of a legislative rather than self-regulatory approach to privacy. On the other hand, that very reliance on government makes people fearful of expressing themselves, that is, they suspect that if they express a view contrary to government policy that there may be repercussions for themselves or their family. Thus, the privacy of communication of expression seen as necessary for the development of democracy is not broadly manifested despite the high value placed on privacy itself.

Privacy protection is also necessary for optimal national development as it would erode the current prevalence of a culture best expressed in the western catch-cry, ‘it’s not what you know, but who you know’. The widespread use of which also demonstrates that this not solely a Jordanian or even

developing world problem, but an international one. The extent of the corruption of processes as universal as access to education, advancement, even medical treatment or social security by considerations such as extended familial loyalties that are irrelevant to optimal national progress (and may indeed be counterproductive) is widely recognised. In a country that values privacy but also familial ties and loyalties expressed in a degree of reciprocity, a greater recognition of privacy rights, while enhancing transparency where required, appears crucial to maximise economic progress and prosperity.

The author believes that informational privacy rights and their role in a just society need to be publicised throughout the Jordanian society in order for such concepts to flourish. Even small changes in practices — such the use of anonymous numerical identifiers for exam situations — could serve to break a current corrupt but widespread practice that impedes the creation of a modern progressive state by continuing to reward familial allegiances in situations where perpetuating such favouritism is contrary to the interests of the state.

The United States appears to place an even higher value on free communication of information as a necessity for a flourishing market and to facilitate democracy than on the privacy rights of persons. US legislation tends to be enacted following specific abuses or problems rather than acting in anticipation of such problems arising. This has led to a very piecemeal approach where the specific situation shapes the legislative response, rather

than — as in a rights based approach — the right shape the legislation and response in advance of a situation arising. Again, as this chapter documents, the US attitude appears predicated on the view of informational privacy as a ‘property right’ and as such able to be bought, sold and transferred, and its contrary right ‘freedom of expression’ necessary for economic prosperity and the growth of democracy. Despite US privacy protection being extended to a number of areas (generally after difficulties have arisen, for example in relation to health information), the US view reflects a somewhat materialistic view of life, contrary (some might say) to Islam where privacy is more viewed as an intensely identity/family related concept, a right not so much to be ‘owned’ as to be ‘protected’. Indeed, in Jordan cultural values such as honour, reputation, democracy and freedom of speech are influenced by the extent to which privacy is preserved and protected.

Whilst the individualism of the US is inimical to government intervention and tends to favour a market-based and private enterprise approach of self-regulation, viewing this as tending towards the good, and only reluctantly introducing legislation where distinct problems arise, the contrasting EU approach embraces a more ‘rights based’ approach, which appears to have more in common with Islam and reasons from the basic ‘right to privacy’ to the issue at hand, an approach inherently more generous in its potential application. However, the long history of US aid may be seen as placing some pressure on decision-makers to at least consider its approach. The counterweight to that is that Jordan and the EU have a similarly long history of interaction culminating in the signing of the *Jordan-European Association*

Agreement,¹ which again brings Jordan into contact with European concepts of privacy and its protection. Substantial trade links Jordan with both the EU and the US ensure that neither is advantaged in regard to determining the nature of any privacy protection measures to be introduced.

The recognition and protection of the right to privacy is crucial to Jordan achieving a number of its objectives: namely, promoting democracy, protecting freedom of expression, maintaining transparency, and combatting corruption and crime. It also offers psychological and sociological advantages as well as economic and political benefits. These can only be achieved with a greater access to informational privacy than is possible under current legislation.

An examination was conducted of the various regional and international instruments and their role, potential or actual, in Jordanian development. Little is relevant and binding, most is advisory at best; much is inapplicable, though perhaps able to serve as a point of reference or model for future national legislation.

The *Universal Declaration of Human Rights* (UDHR) (with Jordan a UN member since 1955) and the *Cairo Declaration on Human Rights in Islam* (CDHRI) exert a moral power only and are not binding on signatories. The *International Covenant on Civil and Political Rights* (ICCPR), on the other hand, is a binding treaty to which Jordan is signatory. It has provisions in relation

¹ EURO-Mediterranean Agreement: establishing an Association between the European Communities and their Member States, of the one part, and the Hashemite Kingdom of Jordan, of the other part, Official Journal of the European Communities, L129/3, Vol 45, 15 May 2002, <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:129:0003:0165:EN:PDF>>.

to privacy and reputation, and privacy of correspondence and family that have specific relevance and could perhaps be further developed. This last also involves a treaty body to which Jordan must submit reports. The ICCPR offers some encouragement to a further extension of privacy rights in the Jordanian context. The *European Convention on Human Rights* (ECHR) offers a model with provisions tested in the European Court of Human Rights. Jordanian citizens may be able to claim some protection in the event of breaches, but in any event it adds further support to calls for domestic legislation and may influence the shape of that legislation.

The chapter also examined the *OECD Privacy Protection Guidelines* which seek to protect personal data and set out eight principles for member countries. While they appear most worthy (embracing collection limitation, data quality, guarantee of purpose and use limitations, consents, security safeguards, transparency and accountability), they are not legally binding on members. They also strive to facilitate the free flow of data between members and specify circumstances where restrictions may be applied. (The OECD also asks that data collectors create codes of conduct.) Again, the OECD Guidelines are recommendations only, which the OECD has no power to enforce. Voluntary in nature, the Guidelines are seen as flexible, but also as reflecting the economic concerns of the body rather than the privacy needs of persons. The *APEC Privacy Framework* with its nine principles was developed from the OECD document but remains advisory only and indeed is weaker than the national legislation of some of the APEC member nations.

Unlike the weaker OECD Guidelines and APEC Framework documents, the UDHR and the CDHR emphasise the right to privacy as a fundamental human right. Thus they are far more consonant with the value placed upon privacy in the *Shari'ah*, and perhaps could therefore be considered more likely candidates for consideration as a basis for domestic legislation. Able to examine the various models, Jordan is well-placed to develop its own privacy approach, one based upon privacy as a human right and taking into account its own particular social and cultural situation as country of Islamic heritage and practice.

Chapter 3 – Privacy in Islam. As Jordan is a country which privileges Islam and regards the *Qur'an* as of Divine origin and the ultimate source of its law, any study without reference to the position of privacy within Islam and Islamic Law (*Shari'ah*) and their major source documents — the *Holy Qur'an* and *Sunnah* — would be irrelevant (and culturally, sociologically, legally, and academically unsound) because Islam, and more specifically the *Qur'an*, is the heart and soul of the people and the State. In this overwhelmingly Muslim country, it is their ultimate guide in all matters. (The Civil Code, for example, is founded on the principles of *Shari'ah*). Importantly, the *Shari'ah* considers privacy as a fundamental human right with many verses in both the *Qur'an* and *Sunnah* able to be quoted to support the concept. Privacy is regarded as part of the human being's inviolable right to dignity. Although extracts appear to address only certain aspects of the right to privacy, this does not mean that the right to privacy in Islam is restricted only to those aspects. Relying on analogy, such a right is able to be extended to new

aspects that have accompanied the ICT explosion. Hence, prohibitions against violating the privacy of the home by trespassing, espionage and eavesdropping, or against violating the obligation to keep private communications of others within the marital relationship, or material imparted in confidence to another, have been extended to cover a broad range of communications and situations. As a general instruction to all people, principles in Islam are seen as applying to public and private entities as well as to individual conduct. It is not a religious or personal matter; the right to privacy of the individual is to be observed by all. The government as well as the people must observe the principles related to privacy that are expounded in the *Qur'an*, the *Sunnah*, and *Shari'ah* principles, neither the highest nor the lowest is exempt.

The belief in the sanctity of the home in Islam serves to provide protection to the intimate nature of people's personal lives and privacy of individuals; it is not seen as a 'property right'. Many too are the injunctions against slander, defamation, gossip and rumour — a reflection of the Islamic belief in the honour and dignity of the person, and the need for its protection, and the need to maintain the basis of trust, mutual respect and transparency in relations. In terms of privacy protection, the injunction against viewing another's correspondence without their approval is seen as tantamount to espionage; speaking ill of another (in their presence or, far worse, not) whether ill-founded or otherwise is not viewed lightly. The damage to individuals, relationships and to the community in general is recognised.

Confidential communications (between spouses or others more broadly) are also subject to bans on disclosure, according to a number of *Hadith* (sayings of the Prophet (pbuh)). An examination of existing codes and policies governing matters of confidentiality and their treatment for Jordanian businesses are based on *Hadith*. This serves as an example of the modern application of traditional principles or their continued development in response to the changing environment.

The author believes that such principles from the *Qur'an* and *Hadith*, and *Shari'ah* principles are able to be expanded to meet issues as they arise. That privacy is treated as a fundamental human right in Islam means that it is also applicable to non-Muslims, their dignity also is to be respected and so similar rights to privacy (as outlined above) exist for them. It also grants a broader brush approach than when privacy is expressed purely as a property right. The *Shari'ah* on privacy provides moral advice and religious guidance alongside legal injunctions and makes respect for the privacy of others an integral part of the social and cultural ethos of the Muslim community. This in turn can be expected to play a supportive role for legislation that may be deemed necessary to guard that right in the modern world.

Chapter 4 – Privacy and ICT in Jordan: The Public Sector. ICTs have been widely seen as providing government agencies in Jordan with the opportunity to improve the operations, efficiency and cost-effectiveness of public services, including education and health, sometimes with the help of aid programs as was the case in relation to the launch of investigations into

the adoption of a national e-Health program 'Hakeem'. Hakeem will be used to establish an e-Health record for residents, keyed to their national ID number and accessible at multiple-points across the health system, and so optimise workflows and reduce patient/medication error rates and the overall costs of health service provision at public facilities in Jordan.² The creation of such databases (only possible with the adoption of new technology), also multiplies the opportunity for the integrity of such data to be compromised unless safely secured from unauthorised or even inadvertent access. The need for the possibility of correction of any errors that may occur also arises.

Other government initiatives have included: the 'e-Village Project', designed to increase access and IT skills at village-level, particularly among rural women; the 'Connecting Jordanians Initiative', which included a plan to place computers in every school, and provide internet access and relevant teacher training (the last UN assisted); and the 'Laptop "Note Book" for every university student' initiative. This last aims to provide such equipment at an affordable price and so help transform the learning environment and bring it into the 21st century, while supporting further growth in the rapidly expanding tertiary education system, where Jordan is already foremost in the region for technological graduates. It should be noted that the extension of the initiative to children as young as 13 has provoked increased concern regarding children's online privacy, given the absence of legislation in that area. Other initiatives include the Broadband Learning Network with its e-

² For progress update, see Electronic Health Solutions website: EHS, *Hakeem* <<http://www.ehs.com.jo/node/70>>.

Learning opportunities, and the broader development of the e-Government initiative. However while all government ministries are accessed via the one e-Government portal, each ministry and government agency is still responsible for the development of its own ICT policies (despite the Ministry of ICT being charged with setting telecommunications policy and strategic planning). The existing lack of privacy protection, however, might deter people from making use of the facilities available.

A case study was conducted in June 2009 involving 40 Jordanian government agencies with an online presence in an attempt to assess the level to which the privacy of personal information is protected by those agencies. The e-Government portal was selected, as this was the entry point for government agencies with the ability to collect, process, access and transfer personal data. Note was made of whether a privacy policy or statement was detected on each connected entity's site. If so, this policy was then evaluated against the 'Fair Information Practices' principles (used by the OECD in the creation of its Guidelines, and adopted by the US e-Government portal that has been ranked by the UN as the world leader in e-Government readiness, and furthermore being refined by the US Federal Trade Commission for the Safe-Harbor Principles). These Principles comprise: (i) *notice* given of site policy prior to consent being given so as to create awareness and the possibility of informed consent; (ii) *consent*, where individuals are to be given an option to determine the use of data collected, including further use perhaps unrelated to the initial reason for collection; (iii) *access*, the right of the person supplying the data to access information collected, ensure it is correct, and

their right to have data amended in the event of an error; (iv) *integrity/security*, where data is to be accurate and secure; (iv) *enforcement/redress*, the existence of effective sanctions embedded in legislation, without which principles remain advisory rather than obligatory, with a lower degree of adherence to be anticipated.

Of the 40 government entity websites accessed, only three (the official e-Government website, and those of the Telecommunications Regulatory Commission (TRC), and Royal Jordanian Airlines) had chosen to place a privacy policy/statement on their sites. It is assumed that this reflects their desire to do so, for if it were compulsory, the other government websites would have complied. As anticipated, the policies varied (for example, in relation to the nature and use of 'cookie' technology, the e-Government and RJA website policies differed, while no notice was posted in regard to such technology on the TRC website). Terms were adopted that had no origin in Jordanian legislation. (The TRC definition of personal information, for example, appeared to have been transposed directly from a US law.) Again, all three are not legally binding policies due to a lack of legislative basis.

While all agencies have the ability to collect data, none (not even those with a privacy policy) offered individuals an opportunity to give or withhold consent to collection nor to further (and perhaps unrelated) dissemination. In respect to the principle of access, only the TRC website grants the right to access own information to ensure accuracy and advise the agency of amendments required. In terms of the principle of security, all three claim to

take 'all reasonable steps' to ensure information is accurate and up-to-date and that superseded material is to be destroyed, deleted or converted to an anonymous form. Finally, in respect of the principle of enforcement, only the TRC privacy statement announced that Jordanian law would govern any disputes arising from the use of the site. None provided clear information regarding complaint procedures or remedies available. No privacy rights enforcement agency exists, so the policies are in effect are little more than 'paper' (the enforcement provision on the TRC website relates to the use of the website rather than its privacy policy).

In the absence of a privacy policy/statement, the vast majority of government agencies (37/40) can still use and disclose personal information supplied to them. As the law stands, they are under no obligation to provide statements of their information practices. The use and disclosure of data could easily occur without an individual's consent.

The situation is made worse by the absence of privacy impact assessment, which could have identified potential problems before they arose. Again with no legislative requirement for such assessment, it does not occur, to the detriment of the developing systems of e-Government and those whose information is being collected and stored, used and transferred.

Overall, while the adoption by government of ICTs accelerates and becomes all-pervasive as government seeks to provide additional services and remodel existing services to take advantage of the benefits offered by ICT (so as to be able to provide services to Jordanians irrespective of their location, economic

status or education), legislation has failed to keep pace with the threats to privacy that accompanies the use of such technology. Indeed the issue of individual privacy has not been addressed by policy makers when they were (and are still) planning and now implementing e-Government. The vast majority of agencies collect and utilise personal data, without addressing the need for guidelines or policies to protect individual privacy. Those few policies (four) which do exist are limited in their application and inconsistent one with the other. As Jordanians become aware of the privacy implications and risks of supplying data, their readiness to use technology and cooperate may be threatened. The situation must change. Currently, it can be summed up succinctly: no legislation, no consistent policy, no enforcement agency – no real guarantee for the protection of personal data.

Chapter 5 – Privacy and ICT: The Private Sector. In recent decades the private sector has grown immensely in Jordan, largely due to the adoption of a policy of privatisation which has seen a number of formerly government owned entities become corporatised and listed on the exchange. Jordan's accession to the World Trade Organisation and signing of trade agreements with important trading partners, such as the EU (the *Jordan-European Association Agreement* (JEAA)) and the US (the *Jordan US Free Trade Agreement* (JUSTFA)), has signalled a new outward looking approach and a willingness to welcome foreign investment. (This was in part a continuation of the policy of trade liberalisation agreed to by the government when the IMF and Jordan entered into an agreement to restructure debt in the wake of crises of the mid to late 1980s).

The trade liberalisation demanded by the WTO General Agreement on Tariffs and Services (GATS) resulted in new legislation to reflect the new trade environment. In the communications sector, market access was increased, foreign participation and ownership broadened, and under the WTO Basic Telecommunications Agreement, the government communications service provider monopoly ended, anti-competitive practices were banned, and a regulatory body established.

In the banking sector, WTO GATS obligations included acceptance of foreign ownership in the sector, a 'level playing field' for transactions and services, increased competition and the entrance of more foreign players.

No consideration appears to have been given in the formulation of the relevant legislation for both sectors to the need to protect the privacy of personal data. The priority appears to have been attraction of foreign capital and alleviate the then economic crisis. A legacy is that the country's depositors, in the banking sector; for example, are able to have their information transferred unfettered across national boundaries.

Capital inflows have helped fund rapid ICT development.³ With private capital inflows, the telecommunications sector now boasts a sophisticated level of infrastructure and is continuing to expand. Liberalisation of the sector has seen increase technology uptake and reduced costs. Internet penetration is about 30 per cent with room for massive growth, which is

³ The national telecommunications provider was the first enterprise privatised. Jordan was also the first Arab nation to fully privatise this sector.

anticipated and is being actively facilitated by the government. Mobile phone penetration is already above 100 per cent, and still growing. Yet little appears to have been done in relation to privacy protection.

A study utilising empirical analysis was conducted of the banking and telecommunications sectors, selected due to their importance and rapid adoption of the use of ICT to collect, store, access and transfer huge quantities of personal data on a routine basis. They were also selected due to the fact that many in these sectors are affiliates of foreign companies and so will illustrate transborder issues. Again information was collected regarding the presence or otherwise of privacy statements/policies on their websites.

The telecommunications sector sample numbered just nine; the websites of the remaining licence-holders either were unable to be accessed due to technical difficulties with their site or they lacked a privacy statement. The privacy statements are evaluated against the FIPs Principles. All providers studied collected personal data. Information regarding their data privacy practices was headed either 'privacy policy' or 'privacy statement'. In terms of notice, 78 per cent contained some form of notice. In regard to consent, 56 per cent provided the opportunity to indicate whether the information collected could be disclosed to third parties. In regard to access, 55 per cent gave participants the right to access their material (companies also provided information regarding how to have material amended). In regard to accuracy/security, companies often advised users on actions to safeguard their material (for example, changing password). In regard to enforcement,

none of the companies offered any information regarding access to an independent agency to help enforce privacy rights. Variations in policies can cause confusion.

The banking sector online case study was conducted in September to December 2009. Of the 23 banks operating in Jordan, 18 (74 per cent) offer online services, the same 18 offer e-banking services. Of the local banks, just 30 per cent (4) have an online privacy statement/policy, as do 37 per cent of foreign banks (3) while neither of the 2 Islamic banks do.

Inadequate disclosure or poor placement by banks of their personal data use policies disadvantages individual customers who neither know nor are able to exercise rights. Such practices include placing a policy on a homepage policy link but not on the page where a credit application is made.

Privacy is further potentially compromised by the globalised nature of banking in Jordan as transborder flows of information become increasingly common. Information is not exchanged just between banks within Jordan but, given the increasing level of level of foreign ownership and number of international transactions, beyond the country's borders to countries where levels of protection may be less than that of the Jordan (or greater, as in the EU).

An online study was conducted in November 2009 on the practices of the eight foreign banks — operating in Jordan and having an online presence — to determine whether or not information collected is shared with third

parties, and whether it is transferred outside Jordan. It is assumed that as e-services are offered, personal data is collected; the question remains only whether it is shared and with whom. Possible answers included other domestic banks and other entities locally, as well as foreign branches or the head office of the bank in question or other entities overseas.

The study found that just three of the eight foreign banks had a privacy statement/policy; each indicated that they shared information with third parties; and one of the three noted that it also transferred information outside Jordan. In the absence of privacy statements by four of the remaining five banks (the fifth being inactive at the time of the study) makes any assumption about information sharing and transfer unsafe. The same can be said in regard to transborder flows. It is however certainly possible, and probably likely, that information is being shared with third parties domestically and information being transferred outside Jordan in the absence of any legislation controlling such activities.

Chapter 6 - The Legal Landscape of Privacy Protection in Jordan. Unlike the US and the EU, Jordan has no specific law or regulation to address violations of individual privacy, although individuals may rely on some sections of some legislation to do so.

The *Constitution* contains some broadly relevant provisions that protect the sanctity of the home (Article 10) from intrusion unless such intrusion is sanctioned by law. The author believes that the Constitutional provisions are insufficient to protect privacy from being invaded via telemarketing.

Likewise, Constitutional provisions to protect the privacy of communications (unless contrary to the law) may also be inadequate to cover private matters (perhaps those irrelevant to the matter targeted) uncovered during legal investigations. Also in question is whether email and other modern forms of communications (Facebook messaging and so forth) would be covered by the Constitution's now antiquated terminology.

Although the National Centre for Human Rights Law was established in 2006, its first report addressing human rights (issued two years later) did not include any specific reference to the right to privacy among the almost 30 human rights related issues mentioned. The concept is not yet 'on the radar' in Jordan.

While the 1976 *Civil Code* mentions violation of 'natural personal rights' without further elaboration, the author believes that this can be understood to include privacy, because privacy must be included in such rights as it is included in the *Qur'an*. Again. Without specifically detailed provisions, the protection may be inadequate if a matter were taken to court.

Penal Code No 16 of 1960 contains relevant material for privacy breach related to slander, libel and contempt which may stem from privacy breaches; while in regard to unauthorised entry to the home or to one's business or private affairs (regardless of the location), charges could not be laid in terms of a 'breach of privacy' without specific provisions being incorporated.

Jordan's citizens may have a right to access their information under freedom of information provisions legislation enacted in 2007, but there is no legislation to protect their privacy. Paradoxically it is the *Freedom of Information Act of 2007* that may offer some hope. Article 10 prohibits the request of information containing data that may be used as a basis of discrimination; while Article 13 forbids the release of government records where such a release would constitute an unwarranted invasion of privacy (including medical, banking, and educational records held by the government).

Problems with the above legislation include: no requirement for a privacy policy or its disclosure, third party transfer is not covered, nor is the use of information accessed. Nor is a hierarchy of interest established in relation to personal privacy and the public interest.

The laws concerning individual privacy in Jordan are marred by a number of shortcomings. First, most of the major laws discussed in this chapter have neglected the right to privacy; the right to privacy is not included in the existing legislation. This is due to the fact that most of these laws were enacted long before the new technologies emerged to play a central role in bringing the issue of privacy into the spotlight. Second, the laws concerning telecommunication and banking sectors were enacted as result of Jordan's commitment to multilateral and bilateral trade agreements. The intention of the telecommunication and banking laws is to facilitate the free flow of information rather than to restrict the flow of information by enacting

privacy laws. Third, the Jordanian legal system lacks of laws and regulations to address privacy issues arising from the new technologies. Children's online privacy, and issues related to surveillance and smart card technologies are yet to be regulated. There is an urgent need to protect individual privacy in this context, particularly the privacy of children.

Finally, Jordan's legal system has avoided implementing a comprehensive privacy protection law, believing that self-regulation is a better approach. This position has been influenced by the US approach to privacy protection. The US influence is quite apparent in the strong political and economic relationship with the US. Jordan adopts similar laws and regulations to those in the US in relation to a number of issues. For example, the latest law enacted by Jordan is the *Credit Information Law of 2010* which is identical to the US law, the *Fair Credit Reporting Act*.

The author believes that Jordan is unnecessarily limiting itself by referring only to the US model and stands to benefit greatly from examining the approaches adopted by other similarly advanced jurisdictions in relation to information privacy and other matters. This includes the European Union model.

Chapter 7 – The Legal Landscape of Privacy Protection in the United States.

Privacy protection in the US legal system reflects the US view of privacy as a property right rather than a human right. It is an approach driven essentially by business interests. The United States champions the 'free flow of information' as conducive not only to the growth of democracy but also to

national economic growth and, therefore, the greater prosperity of the nation, and appears to fear that privacy laws or data protection laws may damage the national economy. An express right to privacy is not among the rights embodied in the *US Constitution*. Nevertheless, the US Supreme Court has held that individuals may have at least a limited constitutional right to privacy (First, Fourth, and Ninth Amendments); however, these constitutional rights apply to individual privacy only against government intrusions, and not those by the private sector. The balance tends to fall towards freedom of expression rather than toward privacy. Informational privacy under the First Amendment also applies only when the government is involved. The Court has also stated that the privacy right available under the *Fourth Amendment* (a prohibition on unreasonable searches and seizure) has little application outside of the context of the investigation and prosecution of criminal activity. The same Amendment restricts government from interfering with private property, ensures compensation for unwarranted government intrusion, provides for due process, and protects citizens from self-incrimination.

Second, the restriction on government actions concerning individual privacy under the *First Amendment* to government legislation and regulations implemented by and for government and governmental agencies has led the US government to rely heavily on the private sector implementing self-regulatory mechanisms for privacy protection within this sector. The FTC report to Congress claimed that self-regulation was the ‘most efficient and

the least intrusive measure to ensure fair information practices online’,⁴ including full implementation of measures designed for privacy protection in information and communications technology area.⁵

The author believes that while it may be the ‘least intrusive’ measure, it may not be the most effective as, in common with all self-regulatory arrangements, it tends to lack enforcement measures, sanctions and so forth, and necessarily tends to reflect the interests of business entities rather than those of the people at large. Stricter requirements were only introduced with the Safe Harbour Principles (derived from the EU mechanism) and to which only those businesses who wished to participate in that market needed to adhere, even then a major concession was made to ensure US acceptance — namely that those breaching the Principles would be subject to prosecution in the US and not the EU.

The US has no comprehensive federal legislation applicable to informational privacy in either public or private sector. Law has been formulated in response to situations as they have arisen and as such is piecemeal. Despite the Federal Government being the world’s largest collector and user of information, controls on its information practices are limited. The 1974 *Privacy Act* is the keystone, instituting consent to collection, maintenance and dissemination practices, and permitting rights of access and correction. However its application is to Federal (not state or local) agencies. It also

⁴ Federal Trade Commission, *Self-Regulation and Privacy Online*, Statement before the Subcommittee on Communications (Committee on Commerce, Science and Technology, US Senate (27 July 1999)

⁴.

⁵ Ibid.

contains a substantial loophole permitting any 'routine use' (including information transfer), if disclosure is 'compatible' with original use. This was partly closed by the *Computer Matching and Privacy Protection Act* of 1988 (CMPPA), making it possible only when written agreements were in place between the agencies in regard to use of the material. No action is now permitted by a third party agency unless the data has been independently verified. But there is no overarching authority provided under the CMPPA. Little redress remains available for violations if they occur.

The relationship between the Privacy Act and the FOIA (and the E-FOIA) is complex but, essentially, where the FOIA requires disclosure, the *Privacy Act* cannot prevent that release; however, the privacy exemptions (for example, in regard to medial and personnel files) of the FOIA can limit the material supplied. Nevertheless, once information is in the public domain, there appears to be no 'clawing it back', even if release was inadvertent or ill-advised.

And whilst laws continue to tighten on government actions, the most recent being the 2002 *E-Government Act* (which requires a Privacy Impact Assessment, adherence to the relevant guidelines and so forth, intrusion in private sector (the business view) or privacy protection (the consumer view) is far less.

The *Electronic Communications Privacy Act of 1986* (ECPA) prohibits unauthorised surveillance of communications by persons or businesses but not against the transactional data generated by the transmissions (for

example, patterns of use) nor its transmission to third parties without disclosing this to the person. Disturbingly, federally only consent of one of the communicating parties is required for a recording to be made (though divulging that information may have other ramifications in law). Interception is allowed when illegal activities are suspected (though warrants would have to be obtained). The ECPA provides both criminal and civil remedies.

A broad recognition of telemarketing as an intrusion, a breach of the 'right to be left alone' led to the enactment of the *Telephone Consumers Protection Act of 1991* (TCPA), an Act where the sheer number of persons calling for reforms to unsolicited calls (telemarketing and faxes of a similar nature) overwhelmed business rights of free expression. It institutes a 'Do Not Call' Registry for the general public and bans calls to emergency services, health care facilities and the like, and includes a private right for damages and injunctive relief.

Children's privacy remains a troubled area. The *Children's Online Privacy Protection Act of 1998* (COPPA) covers only those 13 and under, despite the accepted international definition of a child being a person under the age of 18. Among issues that persist are those regarding reliable identification of the child, and reliable parental consent. However, the rights given to parents in relation to vetoing initial collection, primary or subsequent use and so forth are greater than under any legislation for any other persons in the US.

Privacy in the financial sector is fairly stringently regulated and is affected by a number of pieces of legislation, including the *Gramm-Leach-Bliley Act of 1999* (GLBA), the *Right to Financial Privacy Act of 1978*, the *Fair Credit*

Reporting Act of 1970, the Bank Secrecy Act of 1970, and the institution of the Federal Trade Commission (from 1914).

In summary, US privacy legislation was enacted mainly to address issues involving privacy as they arose, rather than providing detailed, comprehensive protection and this is reflected in their various provisions. The driving force has seemed to be the preservation of business interests rather than the interests of privacy itself.

Chapter 8 – The EU Directive 95/46/EC. Unlike the United States and Jordan, the European Union adopts a comprehensive approach to privacy protection, for which the most significant piece of legislation in this regard is the *EU Directive*. The EU's view of privacy as a universal human right rather than a property right has much in common with the view embodied in the major source of Jordanian law — the *Qur'an*. The EU Directive follows earlier attempts to safeguard informational privacy: for example, the *OECD Guidelines of 1980* and the *Convention for the Protection of Individuals of 1981*, both of which were voluntary guidelines only. The former had no enforcement provisions for OECD member states and the latter could not force compliance by EU member states. Nevertheless both documents served to inform the *EU Directive*. However, the *EU Directive* emphasises privacy as a 'fundamental right and freedom' of natural persons and seeks to protect this, while still encouraging the free flow of information. This contrasts to its predecessors' stronger emphasis on the free flow of information and trade outcomes. Directive provisions exist regarding consent, access and

accuracy/correction provisions exist as do limitations on material able to be shared, explicit rights to object to processing, and, importantly, an active opt-in (rather than opt-out) provision, and remedies.

There are restrictions on transborder flows generally, and more specifically where protection is inadequate. The adequacy of a country's privacy protection is decided on a number of specific elements, including the nature of the data, the purpose and duration of the proposed processing, the countries involved, and the laws in force and professional rules and security measures in place in the third party country. Limited exemptions are provided where consent is unambiguous, and for sales transactions and money order transmissions.

The *EU Directive 95/46/EC* plays a significant role in protecting individual privacy at international level. The EU is also an important partner of Jordan in terms of trade and securing a free trade zone for the two by year 2014 is a priority. It is subject to Jordan carrying out a number of economic, social and political reforms. On the issue of privacy protection reform, Jordan is yet to meet the requirements of the *EU Directive*. Under the provisions that examine the adequacy of a third country's privacy protection, Jordan is currently unable to be listed as an adequate recipient of personal information from the EU Member States. This is due primarily to Jordan lacking legislation that addresses the treatment of personal information in both the public and the private sectors. The (Chapter Four) case study on privacy and e-government determined that the majority of government agencies in

Jordan do not have privacy policies or statements with respect to handling personal information. The private sector in Jordan will also be deemed 'inadequate' as it fails to provide a minimum of privacy protection. Member States will, therefore, prevent the transfer any type of information to businesses in Jordan. The (Chapter Five) case study showed that there is no privacy protection law or guidelines in the area of banking and/or telecommunications industries. These two specific business areas are shown not to provide a minimum level of privacy protection for the processing of personal information.

The United States being in a similar position — unable to guarantee privacy protection under its legislation — has negotiated a compromise resolution under the Safe Harbor Principles, which does not obligate all businesses in the US to adhere to EU standards but only those companies wishing to participate in the market. Its seven requirements appear almost identical to the EU Directive; however 'opt out' is maintained in the choice provision and any enforcement in terms of prosecution is to be conducted in the relevant home country (for example, US companies in the US).

The author believes that Jordan's lack of appropriated domestic legislation is an obstacle to the creation of a Safe Harbour or even more comprehensive arrangement. The issue of 'inadequacy' of privacy protection in Jordan leads to the consideration of possible alternatives for Jordan, and proposals for national privacy policy reform that would allow Jordan to be considered as a

country with ‘adequate’ privacy protections in place in both the private sector and public sectors, and so able to become an ‘adequate’ third party country.

9.3 The Possible Policies for Privacy Protection in Jordan

Based on the above chapters, there are two different regimes available to policy makers in Jordan, a knowledge of which may assist in the evolution of ‘privacy’ as a legal concept. First of these approaches is that of self-regulation (as typified by the US). The following section defines self-regulation and examines its suitability for Jordan. The second of these approaches is that of comprehensive legislation for privacy protection (as typified by the EU). Policy makers in Jordan can call for national legislation for privacy protection that is compatible with the *EU Directive*. The question here, however, is which of these regimes is the most suitable for privacy reforms in Jordan?

This question, and an examination of the alternatives, leads to a proposal for national legislation for privacy protection in Jordan. The proposal seeks to constitute privacy as legal right and to lay down basic guidelines and standards to ensure the protection of this right.

9.3.1 The Self-Regulatory Approach

Policy makers in Jordan, however, are more likely to implement a policy of self-regulation if the issue of privacy arose. This is may be justified on a number of grounds. First: the information and communications technology sectors are encouraged to implement a self-regulatory approach. This has been one of the main tasks of the Jordanian Telecommunications Regulatory

Commission (TRC).⁶ Secondly: the close and sensitive relationship between Jordan and the United States plays an influential role in the creation of a policy on privacy protection in Jordan that would be similar to that of the United States. The idea of self-regulation is well recognised and admired by the US policy makers, who strongly object to the introduction of any comprehensive legislation. The US position, in this context, can be easily observed in the US-Jordan Joint Statement on Electronic Commerce. On the issue of privacy, the statement clearly stated that: ‘governments should encourage effective self-regulation through codes of conduct, model contracts, guidelines, and enforcement mechanisms developed by the private sector’. On the issue of privacy, the joint statement added that: ‘government should encourage the private sector to develop and implement enforcement mechanisms, including preparing guidelines and developing verification and recourse methodologies’.⁷

Further, the Jordan-US Free Trade Agreement has largely contributed to the trend of Jordan following in the footsteps of the United States. For instance, Jordan has recently enacted laws in the field of credit reporting, anti-money laundering and freedom of information which can be seen to be very similar to those of the United States. That the United States appears to have had to negotiate a compromise with the EU in terms of the *EU Directive* with the adoption of the Safe Harbour principles (a perhaps slightly watered

⁶ *Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002*, (Jordan) *Official Gazette* No 4416, 17 February 2000. The original law was issued in the *Official Gazette* No 4072, 1 October 1995, art 6(g).

⁷ U.S.- Jordan Joint Statement on Electronic Commerce <http://www.jordanusfta.com/documents/joint_statement_on_e-commerce.pdf> at 28 August 2009.

down version of the *EU Directive*) may be a reflection of the its emerging economic vulnerability; however, that a compromise solution was found clearly demonstrates its strength has not yet waned to such a degree that the entire nation has to comply to the Directive in order to gain 'adequate' status for businesses desiring to trade in the EU, or that its citizens would be brought before EU rather than US courts for breaches of the privacy legislation. Some would certainly say that the self-regulatory and comprehensive have here met together for a mutually satisfying outcome in terms of both trade and privacy protection in relevant interfaces or areas of interchange.

9.3.1.1 Advantages of the Self-Regulatory Approach

The purer self-regulatory approach remains attractive to business, as they perceive that there are several advantages in implementing the self-regulatory approach rather than governmental legislation with regard to privacy protection. First, self-regulation allows for greater flexibility than government legislation.⁸ It is easier for an industry group or entity representing a profession to alter and modify rules as a result of changing circumstances than for legislation to be amended. Self-regulation is easier to design to suit a specific business than is government legislation.⁹ Further, self-regulating privacy in information and communications technology requires fewer procedures in order to encourage innovation and provide

⁸ Julia M Fromholz, 'Data Privacy: The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 461, 478.

⁹ Angela J Campbell, 'Self-Regulation and the Media' (1999) 51 *Federal Communications Law Journal* 712, 716.

more choices for individuals. In this context, self-regulation is seen as more flexible than government regulation in achieving this goal.¹⁰

Secondly, self-regulation creates greater incentives for businesses to regulate privacy.¹¹ Often self-regulation staves off the possible introduction of government regulation, which is generally perceived by business and others as likely to be more onerous, complex and less business friendly than a mechanism largely designed by the industry, business or professional sector itself. In order to create such an incentive, specific codes and/or guidelines that could jointly adopted by businesses and their customers and enforced through private mechanisms must be created by the sectors.¹² It is also more likely that business and industry will respect and comply with codes and guidelines that have been developed internally rather than codes imposed from 'outside'.

Thirdly, self-regulation has the potential to utilise greater expertise and technical knowledge that can only be provided by those in a particular industry or business sector. Internally developed regulations may be able to be formulated in such a way that its provisions are able to be interpreted accurately and unambiguously within the industry or business sector, thus increasing compliance. This may reduce the costs that might otherwise result from seeking to monitor and enforce these regulations (by whatever measures voluntarily agreed upon in the respective code of practice).

¹⁰ Peng Hwa Ang, 'The Role of Self-Regulation of Privacy and the Internet' (2001) 1(2) *Journal of Interactive Advertising* 76, 81.

¹¹ Campbell, above n 9, 716.

¹² Catherine Louisa Glenn, 'Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records' (2000) 53 *Vanderbilt Law Review* 1605, 1630.

However, any costs arising in this context will be borne by the relevant business or activity.¹³ Finally, the flow of personal information is the foundation on which businesses can succeed. Many businesses rely on the practice of collection, use and exchange of personal information. The only policy that is acceptable to business to regulate such practice is the adoption of a self-regulatory policy rather than government intervention. Business practices in this area may harm individuals only to the extent of being ‘an annoyance’, which is not considered reason enough to introduce government legislation to address this issue.¹⁴

9.3.1.2 Disadvantages of the Self-Regulatory Approach

In spite the above advantages; there are some disadvantages to self-regulation as a policy for privacy protection. The primary shortcomings of self-regulation in the context of privacy are: (1) the lack of enforcement, and (2) the question of the availability of legal redress for individuals harmed.

On the issue of enforcement, a self-regulation policy is lacking proper mechanisms to enforce rules and codes of practice. This is due to the fact that any enforcement mechanism requires an input of effort, resources, and time to monitor businesses’ practices internally and a mechanism to submit the results to an overarching industry body or organisation created under the voluntary code and supported by the respective industry members. This will generate significant costs to businesses. In most cases, efforts will not be

¹³ Jose M A Emmanuel A Caral, 'Lessons from ICANN: Is Self-Regulation of the Internet Fundamentally Flawed?' (2004) 12(1) *International Journal of Law and Information Technology* 1.

¹⁴ *Ibid* 5.

sufficiently funded,¹⁵ neither for the internal monitoring required nor for any external review by an industry body. Further, because self-regulation policy is voluntary and lacks adequate enforcement mechanisms (if any), some businesses — for the sake of greater profits — will not comply with (or will fail to fully comply with) any rules or codes of practice created. Those businesses that do comply will be placed at a competitive disadvantage, which in turn may disadvantage individual businesses in the particular sector and owners and employees of those businesses.¹⁶

Therefore, without a strong commitment to ensuring an obligation to comply with rules and codes of practice, self-regulation is considered to be inadequate as a policy to provide the protection needed for personal privacy.¹⁷

On the issue of legal redress, when a business breaches its own rules of practice, individuals who harmed as a result of this breach may not be able to seek compensation. Businesses providing rules and guidelines rarely offer individuals meaningful channels for compensation in case of member

¹⁵ Ya-Ching Lee, 'Will Self-Regulation Work in Protecting Online Privacy?' (2003) 27(4) *Online Information Review* 276, 280.

¹⁶ Campbell, above n 9, 718.

¹⁷ Deidre K Mulligan and Janlori Goldman, 'The Limits and the Necessity of Self-Regulation: The Case for Both' in 'Privacy and Self-Regulation in the Information Age' (U.S. Department of Commerce, 1997), <http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm>.

For instance: TRUSTe is a major seal programme that promotes privacy practices. It represents one model of the adoption of a self-regulation policy. Large businesses sponsor the TRUSTe seal programme as their privacy policy, but that does not necessarily mean that they comply with its guidelines which, after all, are voluntary. For example, in spite of Microsoft being a corporate sponsor of TRUSTe, it does not comply with the TRUSTe privacy guidelines. When Microsoft was criticised for monitoring customers' actions, TRUSTe did not conduct audit proceedings on Microsoft's privacy practices. This weakens the credibility of the TRUSTe programme. Further, not all the TRUSTe sponsors subscribe to the programme and license the logo.

violations.¹⁸ If the business cannot be held liable and the affected individuals cannot seek a remedy when a violation of self-regulation policies occurs, the incentive for a business to adhere to policy diminishes.¹⁹

Furthermore, and most importantly, self-regulation leads to the empowering of certain groups (for example, business lobbyists), which are not accountable through constitutional channels. A conflict may arise between these groups and constitutional bodies.

As a result of privatisation in Jordan, the many governmental bodies have been created (commissions and the like) with the task to regulating and monitoring relevant particular industries have been delegated full power for rules-making, adjudication and enforcement. However, these commissions appear not to be subsequently accountable to any constitutional authority (in this case, the Parliament) and act with unfettered power and ostensible lack of regular parliamentary review. The lack of accountability and transparency in the rule-making process is considered to be a drawback to democracy in Jordan and consequently a setback to the introduction of a regime of protection for privacy rights.

The TRC is one such commission with many powers delegated to it as the regulatory authority in regard to telecommunications law and the self-regulatory approach broadly preferred by industry. Existing privacy policies in Jordan are not generally effective in providing adequate protection for

¹⁸ Mulligan and Goldman, above n 17.

¹⁹ Jonathan P Cody, 'Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation' (1999) 48 *Catholic University Law Review* 1183, 1225.

informational privacy. Self-regulation may be work effectively when there is a very high level of awareness, among individuals and businesses alike, of the concept of privacy; but in Jordan this is not the case.

To a great extent individuals believe that the government, and only the government, will protect them from any violations to their privacy by those in the private sector. Secondly, the idea of self-regulation, similar to the concept of privacy, is yet to fully evolve. As demonstrated in earlier chapters, most businesses that have online presence in Jordan do not pay a great deal of attention to privacy. In relation to other businesses, which do have privacy policies, such policies are usually 'unintelligible', full of 'electronic boilerplate',²⁰ and, most importantly, were generally imported from abroad rather being 'Jordanian made'. They therefore suffer from a lack of genuine comprehension of the specifically Jordanian context in which they operate.

9.3.2 The Comprehensive Approach

The second approach that could be available for policy makers in Jordan is to implement comprehensive legislation for privacy protection similar to that implemented in the EU rather than solely implement self-regulatory measures. In the context of Jordan, this approach has many advantages over the self-regulatory approach outlined above.

First, and most importantly, government legislation will define the concept of 'privacy' as a legal term, taking into account social and cultural issues. As has been mentioned above, the concept of privacy in Jordan appears on the

²⁰ Kamaal Zaidi, 'Harmonizing U.S-E.U. Online Privacy Laws: Toward a US Comprehensive Regime for the Protection of Personal Data' (2003) 12 *Michigan State Journal of International Law* 169, 186.

surface as a major issue only in regard to two important aspects of the Jordanian society that are seen as requiring special protection: family and/or women. This is simply because Jordan, as a predominantly Muslim country, privacy protection of those two areas is inherent in the faith and the principles of Islam. As discussed in Chapter Three, Islamic Law (*Shari'ah*) has on many occasions explicitly protected the privacy of family and women. In light of ICT advancements, and given the sensitivity of these two aspects of Jordanian life, explicit privacy protection in the form of government legislation is the most appropriate form for ensuring this protection. Such legislation may lead to recognition of the value of privacy, not just for family and women, but as an important value as a whole.

Secondly, the Government of Jordan (GOJ) is the 'sole player' in the country in terms of being the largest single employer and, as government, the chief source of legislation and regulation. It has played an essentially paternal role, looming far larger in the lives of the people than many governments elsewhere (particularly in the US). Since the foundation of Jordan in 1923, the Government undertakes the responsibility to guarantee individuals' needs in every aspect of their lives. Further, individuals are relying on government to provide them with services and address their problems. This contrasts strongly with the individualistic, self-reliant, competitive and far less government interventionist approach traditionally characteristic of the US, but to a far lesser extent in Europe, especially northern (socialist welfare state) Europe.

One important role that individuals expect all governments to play is to introduce, amend, and repeal legislation. In Jordan, however, the level of dependence on government makes people look to government perhaps more often than elsewhere for solutions to problems. In the area of privacy, individuals believe that government legislation is the best approach to the protection of their privacy as the idea of self-regulation is yet to be understood and accepted by them.

From the research conducted, individuals where self-regulatory guidelines are the 'tools of choice' seem to have less access to redress where guidelines are breached. This may be understandable as self-designed measures might be far more likely advantage those who design them (industry) than those who may be adversely affected by measures that business would otherwise see as less conducive to 'their' rights. Thus individuals (as opposed to industry or service providers) in self-regulatory systems may have little or no control in making sure that industry is complying with its own policies and guidelines.

Unlike self-regulatory measures, government legislation is a legally binding and generally accompanied by measures of enforcement in the event of their breach. Industries will be more likely to comply with rules and guidelines stated in the legislation to avoid claims by individuals and penalties imposed by the government. At the time of writing, there was no reported case filed by individuals against any industry in Jordan to make a claim in relation to a violation of business codes of conduct or their guidelines.

Thirdly: comprehensive privacy legislation in Jordan may become commercially worthwhile. The argument that says imposing restrictions on the transfer of information may disadvantage the economy may not be strong enough to justify rejecting the imposition of restrictions, because new concepts such as 'privacy' will be embraced and accepted by the Jordanian society. Just as individuals have welcomed the new technologies, they are willing to welcome 'privacy' along with those technologies, particularly when they become aware of its importance. Further, as new concept, a demand for privacy will become accepted as an essential part of their use of new technologies. Consequently, individuals will search for businesses that have privacy principles in accordance with the government legislation. Businesses are then likely to compete between each other to make sure that their privacy principles meet with this legislation.

Furthermore, privacy legislation in Jordan may attract business opportunities from foreign countries. For example, foreign businesses in the European Union are likely to invest in countries that have privacy protection laws that are compatible with the *EU Directive*. As discussed above, however, Jordan is considered to be a place that does not provide an adequate privacy protection. The adoption of a comprehensive approach to privacy protection in Jordan would permit Jordan to be considered a country that does provide adequate protection and meets the European Union standard on the issue of privacy protection. This eventually, would make Jordan an attractive market

not just for European businesses but also for other countries that have privacy protection laws.

The influence on Jordan of the US self-regulatory approach may not last. This is because the US government remains committed to the privacy principles in the *Safe Harbour Agreement*. This agreement, which meets the comprehensive privacy principles of the *EU Directive*, gives a strong indication that any comprehensive privacy legislation in the US may be increasingly shaped by the privacy standards in the *EU Directive*.²¹ Despite the US strongly favouring a regime of self regulation for privacy protection, the US may support Jordanian policy-makers in their bid to legislate a comprehensive privacy law, at least to deal with the privacy issue in the public sector. Such a law would be similar to the *US Privacy Act of 1974*. However, if the US expresses some sort of reservations on Jordan's implementing privacy law, such reservations would be unwarranted and such a position — if taken by the United States — would be seen as a hypocritical.

In summary, it can be concluded that a regime of self-regulation alone cannot ensure the protection of individual privacy in Jordan. This conclusion is supported by the case studies above, which were conducted in both public and private sectors. Furthermore, a comparison of Jordan and the United States cannot be used to justify the implementation of a self-regulatory approach. It would be unfair and impractical, as there are important cultural, social, economical, and political differences between the two countries. From

²¹ Ibid 186.

a cultural and social perspective, the widely held belief in Jordan that only the government has the legal authority for introducing regulation, would severely hamper the introduction of any system based on self-regulation. Without effective civil institutions and strong consumer protection advocates in Jordan, the burden of regulation continues to fall only on the Government of Jordan. This position is very different to that in the United States. There the lack of trust in government (and a belief in almost unfettered freedom for private enterprise) tends to have led legislators to date to reject all attempts to create comprehensive privacy legislation. Instead, the US legislators adopted a piecemeal regime through enacting specific legislation to address certain issues for specific target areas (as discussed earlier).²² In addition, governmental and (in contrast to Jordan) non-governmental agencies are employed to watch and enforce individuals' privacy rights should there be violated.

From an economic perspective, Jordan has a small economy compared to the United States. The failure of self-regulation if adopted in Jordan would have serious consequences on the whole economy. Its adoption is unlikely because the idea of self-regulation is not yet a part of the local culture and is unlikely to be any time soon in the future. Such a concept would be slow to grow and take a long time to become accepted by the major actors in Jordan, namely the government, the businesses and the individuals. Its adoption would fail, due to one genuine reason — businesses would seek profits without seeking

²² Chuan Sun, 'The European Union Privacy Directive and its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective' (2003) 2(1) *Northwestern Journal of Technology and Intellectual Property* 99, 105.

or gaining individuals' trust and confidence through a privacy protection mechanism. In a culture that respects the authority of central government as the most legitimate and is unaccustomed to self-regulation, businesses are unlikely of their own accord to create regulations that would potentially — and effectively — limit their economic power or their ability to exploit information obtained to their advantage and profit; nor might such self-regulation attract the respect necessary to guarantee a high level of compliance.

In contrast, the idea of self-regulation in the United States is deeply rooted in American culture. This idea is based on the theory that the marketplace will protect individual privacy (and gain individual trust and confidence) in return for greater profits. Again, in contrast, the growth of the free market has been seen by some in Jordan as a source of corruption and higher prices, and subsequent unrest.²³ The 'free market' reforms in themselves are not necessarily viewed as inherently good; appeals continue to be made to the central government to alleviate any detrimental effects.

The political differences between both countries remain another factor for the rejection of self-regulation; it is not seen as the desirable approach to privacy protection in Jordan. Despite the Kingdom's long-reigning and stable dynasty (Hussein 1952–99, Abdullah II 1999–) with its reputation for reform, and increasing commitment to economic liberalisation, privatisation, modernisation of the law and democratisation, there remain significant gaps

²³ Suleiman al-Khalidi, 'Jordan's King Appoints New PM after Protests' *Reuters*, 1 February 2011, <<http://in.reuters.com/article/2011/02/01/idINIndia-54565020110201>>.

(for example, members of the lower house only are elected, the Upper House is selected by the king). In contrast to the apparent stability of the monarchy and although few parties exist, there are frequent changes of government in Jordan.²⁴ The use of delegated powers by a government minister may make policies and guidelines easy to change, delete or amend with any change in government, but the situation is likely to be worse should self-regulation be adopted.

Changes in policies and guidelines are able to be rapidly effected where there is little central government control, in situations where self-regulation exists, where industry itself is the key to the standards of care, codes or rules adopted and their enforcement — or, perhaps, lack of effective enforcement, given that this appears to be frequently encountered where voluntary systems of self-regulation are adopted elsewhere. Voluntary codes are just that, voluntary — with no guarantee of universal acceptance and adherence in any or all members or participants in the required sectors in industry, business or professional body. Intermittent or irregular compliance across an industry or rapid changes to Codes themselves (and to their levels of compliance or enforcement) may cause confusion to individuals and industry alike, reducing consumer and industry confidence.

The best way to avoid such confusion and the disadvantage this would bring to individuals in regard to privacy protection is to bring privacy legislation through the democratic process of the parliament. This would ensure greater

²⁴ 'About Jordan: Government' Jordan Official Site of Jordan E-Government website <<http://www.jordan.gov.jo/wps/portal>> at 5 March 2011.

acceptance of the Code by business, industry and consumers alike, while the availability of state enforcement would encourage compliance. Its passage through parliament rather than announcement by governmental or ministerial fiat would also serve to publicise the Code. The best result —in terms of aptness of legislation and broad acceptance of a state-devised Code — is most likely to occur in the wake of adequate consultations and discussions with the many relevant stakeholders. The following section presents a model for privacy legislation to be recommended to the policy makers in Jordan.

9.4. The Self-Regulatory Approach or the Comprehensive Approach: *The Case of the UK Media Scandal*

9.4.1 Background

The *News of the World* scandal has turned the focus on the issue of whether tougher laws and regulations are needed to protect individual privacy. The overwhelming reaction from the public to this scandal has proven that privacy is undoubtedly — particularly in the ICTs context —a growing concern not just for UK citizens, but also for many people around the world.

A national tabloid newspaper published in the United Kingdom from 1843 until its closure by its owners in 2011, the *News of the World* tended towards the sensationalist, exposing celebrities in unguarded moments, and obtaining stories by deception. More recently, it was revealed that it had perpetrated illegal interceptions of phone calls, including voicemails ‘phone hacking’ for more than a decade. Among targets were ongoing police investigations, and private phone calls of hundreds if not more persons, including the families of

murder victims,²⁵ of UK service personnel killed in action, ‘popstars’, sporting identities and royalty.²⁶ A Royal Commission resulted; and serious charges have been laid in a number of instances.²⁷ Allegations of phone began to surface in 2006. It prompted the UK government first to hold a British Parliamentary Inquiry and then to set up a Commission of Inquiry headed by the Lord Justice Leveson which will include newspapers, broadcasters and social media.²⁸

9.4.2 The Phone Hacking and the Law

Under the UK law, there are a number of laws and regulations address privacy protection and, in particular, phone hacking. First, the hacking into messages on mobile phones is covered by the *Regulation of Investigatory Powers Act* (RIPA) 2000. Section 1 of RIPA 2000 makes it an offence for person intentionally and without lawful authority to intercept any communication in the course of transmission by means of a public telecommunications.²⁹ RIPA 2000 also creates a private right of action for unlawful interception on private telecommunications systems.³⁰

²⁵ <http://news.smh.com.au/breaking-news-world/murder-victims-family-wants-news-exec-out-20110711-1har2.html>

²⁶For detailed material including evidence before the Committee of Inquiry: see UK Parliamentary website <http://www.parliament.uk/business/news/crime-civil-law-justice-and-rights/privacy/phone-hacking/>
<http://www.zdnet.com/blog/igeneration/royal-phone-hacking-scandal-police-to-reveal-victims-names/8452>

²⁷ Stephen Wright and Rebecca English, ‘Editor Charged in the Royal Phone-Hack Affair’ *Mail Online*, 9 October 2011 <<http://www.dailymail.co.uk/news/article-399896/Editor-charged-royal-phone-hack-affair.html>>.

²⁸ Lisa O’Carroll, ‘Phone-hacking Inquiry Extended to Include Broadcasters and Social Media’ *The Guardian*, 20 July 2011. <http://www.guardian.co.uk/media/2011/jul/20/phone-hacking-inquiry-broadcasters-social-media>.

²⁹ *Regulation of Investigatory Powers Act 2000* (UK) (RIPA) ss 1(1) and (22).

³⁰ *Ibid* s 1(3).

RIPA 2000 was enacted to put the covert work of the intelligence agencies and the police onto the statute books and bring their activities into line with the European Convention on human Rights (ECHR). Therefore, RIPA 2000 makes no provision for anyone outside the police and intelligence agencies to obtain authority to phone-tap or hack. Specifically, there is no public interest defence for a person found in breach of RIPA 2000.

Second, the UK *Data Protection Act* 1998 grants powers to the UK Information Commission Office (ICO) to prosecute those responsible persons for unlawfully obtaining, disclosing, or procuring the disclosure of personal information without the consent of the organisation holding the information. However, the lack of resources available to the ICO, make it very hard to proceed with these prosecutions.

Third, Clause 10 of the Press Complaints Commission (PCC) warns that the press must not seek to obtain or publish material acquired by intercepting private or mobile telephone calls, messages or e-mails, or by accessing digitally held private information without consent. Accordingly, a victim of phone hacking may rely on this clause and present his/her complaint about phone hacking by the press to the PCC. However, the PCC may be declined to investigate such claim based on legal grounds as neither the existence of civil proceedings, nor the rules of *sub judice* in criminal cases prevent it from investigating.

9.4.3 Analysis

The author believes that this particular UK media scandal clearly reveals that neither UK privacy protection law nor the self-regulatory approach prove to be adequate to protect individual privacy. The spread of new technologies pose new threats to individual privacy which have outpaced the law. It is almost impossible to stop the spread of these technologies. The only way, however, to deal with this reality is to propose a general right to privacy.

The main purposes of such proposal are to: (1) ensure certainty for individuals to take legal action against anyone for a breach of their privacy; (2) deter individuals, government and businesses from violating privacy. An actionable right to privacy would enable individuals to take action against illegal treatment (collection, access, disclosures and transfer) of personal information; (3) provide an effective way to compensate injured persons of invasions of their privacy. A liability for privacy invasion is necessary to help society as a whole reclaim some of its values, in a world that is so dominant by advanced technologies.

The author also believes that the society should determine the social and ethical standards to apply to the use of ever-changing technology, so valuable information does not fall into the wrong hands for the wrong purposes.

One important benefit of such proposal is that a general right to privacy would provide uniformity. This means that both public and private entities alike would be regulated by one single piece of legislation. In addition, a

general right to privacy would provide a benchmark for effective policies and standards to keep up with changing technologies.

The following sections suggest -as a final thought- a model legal framework to privacy protection in Jordan. A model consists of two legislative bodies: (1) a national legislation to privacy in Jordan and, (2) a national commission to enforce privacy rights. These bodies are examined respectively.

A Final thought

9.5 A Model Legal Framework for Privacy Protection in Jordan

This final section of this research recommends a model legal framework for privacy protection in Jordan. The proposal is a significant attempt by this research to lay down privacy principles at a time of rapid development in information and communications technology (ICT) and a concurrent lack of privacy protection laws in Jordan. It has been concluded, above, that individuals cannot rely on privacy guidelines presented to them through a self-regulation approach. Therefore, individuals seek a national legal framework to protect their privacy and to be applicable to the public and the private sectors. For this matter, the author recommends that the proposed legal framework consist of two parts: first, national legislation for privacy protection to be drafted and implemented, with the proposed legislation to be referred to hereafter as the '*Privacy Protection Law*' (PPL); and secondly, the establishment of an independent national agency for privacy protection in Jordan, with this agency to be cited as the: '*Jordanian Commission for Privacy Protection*' (JCPP). The following section presents the features of the first part.

9.5.1 The Jordanian Privacy Protection Law (PPL)

9.5.1.1 The Scope of the PPL

The proposed *Privacy Protection Law* (PPL) for Jordan should address all types of personal information practices conducted by government agencies and/or private businesses. This is important so that individuals are able to feel confident and secure that their privacy is equally protected on all levels

and in both private and public enterprises and areas of private or governmental activity. If the PPL was to be applicable to certain areas only and to be excluded from other areas, individuals may be confused as they may mistakenly assume that their privacy is protected in the excluded areas. A consistent and universal approach to privacy protection (in so far as is reasonably possible) is highly desirable to minimise such confusion.

The PPL should provide a broad definition of the concept of privacy. It may be difficult to define privacy precisely, but it is possible to regard privacy as ‘a fundamental human right’, consistent with *Shari’ah* and in light of current demands of modern human rights legislation. The right in this context is considered to be valuable and connected to individuals’ identity.

Further, the PPL should define the term of ‘personal information’ and provide a list of types of information that may be used to identify individuals and that is covered by the legislation. For some businesses, for example, the mobile telephone number may not be considered as an item of personal information while for others it is. In order to solve this anomaly, the PPL should include three categories of items that may define the term of ‘personal information’. These categories are: (1) a category for general personal information, which includes: first and last name, date of birth, current and previous addresses and national identity numbers, telephone numbers, and electronic mail addresses, (2) a category for specified personal information, which may include: relative names (parents, siblings and children’s names), employment history, educational qualifications, criminal history, spending

preferences, and marital status; and (3) a category for sensitive information, which may include: general health information, genetic information (DNA), fingerprints, sexual preferences, and political and religious beliefs, affiliations, and aspirations.

The intention from the above categorisation is that each category may require different level of protection to maintain an adequate right to privacy. For example, unlike the first category, the second category of personal information should be subject to special treatment, which would require specific regulations and guidelines. Furthermore, the personal information included in the third category should, when held by the private sector, be subject to more restrictive privacy regulations than if it were held by the public sector, because even though both sectors have the same ability to collect, use, access, and disseminate personal information, the private sector has the ability to transfer this information to foreign countries where Jordanian law has no jurisdiction and so it would be beyond the reach of protection guaranteed in such legislation. Tougher restrictions should be placed on the private sector in the proposed legislation in order to regulate the flow of personal information.

Before discussing individual control of information flow, a second feature of the PPL — the use of a standard notification form and process — will be discussed below.

9.5.1.2 Individual Standard Notice of Information

The proposed PPL requires that individuals are to be informed when all types of personal information is being collected about them by either private businesses or governmental agencies. This can be achieved by giving individuals an explicit 'notice' explaining 'what information is being collected about them, from whom it is collected and how it is collected'.³¹ This can be incorporated both in hard copy written materials distributed to individuals for them to complete and in on-line websites and for a where information is increasingly gathered and is the particular focus of this thesis. To inform those being asked to supply personal information of their rights in relation to these matters, it is recommended that the proposed PPL incorporate a recommendation that a standard notification be drafted in language that is easy to understand by all types of individuals. The standard notification, whether devised by business, industry, professional body or government department should contain identical information to explain privacy practices, and provide similar levels of safeguards. For example, if one assumes that an individual wishes to make multiple applications to obtain a credit card from different credit card providers, he or she should be able to assume that all credit card providers (whether private bank, credit union, or other credit providing facility, such as that provided via a retailer?) are providing the same level of protection to personal information. This assumption would be based on the standard notice given to individuals under the PPL. The 'standard notice' may serve three important goals: first, it gives individuals

³¹ Mark E Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate' (1998) 49 *South Carolina Law Review* 847, 880

the confidence and the trust that their personal information is protected at the same level when dealing with various types of businesses. Secondly, the use of a standard form of notification simplifies the issue of privacy. A 'standard notice' will not be a source of confusion for individuals; they will — at least theoretically — no longer need to read privacy policies or statements for each business as they would be aware that certain contents must by law be contained in such statements, and that a business that breached the legislative requirements would be liable to whatever sanctions were available under the relevant Act. The easy to understand language used would, however, make it more comprehensible and more likely to be read and understood, rather than seen as 'fine print' and 'too difficult'. Further, the existence of a standard notice that contained the basic principles on personal information privacy would help individuals to become familiar with these principles and assist individuals to identify any gaps or shortcomings in an information notice that they might encounter. An increase in such knowledge will be empowering. Individuals will become more active in protecting their own privacy. Finally, a 'standard notice' that is compliant with the PPL will avoid needless costs (generated by uncertainty) to businesses. Should a privacy dispute arise, a business would rely on the interpretations of the PPL given by the court, rather than interpretations provided by private consultants. The court's interpretations would benefit individuals and businesses alike by ensuring certainty and predictability.

9.5.1.3 Individual Choice and Control of Information

The proposed PPL should grant individuals the right to decide whether their personal information is to be used by a specific industry and for which purposes it is to be used. The PPL recommends the right to 'opt in' over the right to 'opt out' in order to maintain the right of choice at a higher level than would otherwise be the case. The recommendation for the PPL to implement a right to opt in mechanism is justified on a number of grounds.

First, an opt in mechanism strengthens the principle that personal information is about the identity of the individuals and only concerns them rather than any other entities. It gives individuals greater control over their personal information on the assumption that they do not want their privacy to be invaded. If they wanted to share this information with others, however, they should have the ability to do so.³² Secondly, an opt in mechanism educates individuals about their information privacy rights. Under an opt in approach, for example, an individual will be given the opportunity to learn whether their personal information is to be transferred to third parties and then be able to make their own choice about it. In contrast, when individuals are given the opportunity to opt out, it is possible that they will miss or inadvertently ignore this opportunity.³³ Thirdly, the adoption of the opt-in mechanism in the PPL complies with the provisions of the EU DirectiveAs stated in the previous chapter, the EU Directive in Article 7(b) has favoured the opt in over the opt out approach. Consequently, the PPL as outlined will

³² Mark E Budnitz, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate' (1998) 49 *South Carolina Law Review* 847, 882.

³³ Jacqueline Klosek, *Data Privacy in the Information Age* (2000) 176.

be considered as an adequate law for privacy protection, one that meets the EU standards.

9.5.1.4 Limited Access

The suggested PPL incorporate a recommendation/requirement that government agencies and private businesses lay down set of guidelines and procedures to restrict access to individuals' information by employees and/or third parties. Government agencies and private businesses which allow third parties to access individual personal information will be found liable in case third parties violate individual personal information. Entities must make sure that the third parties have an adequate measures and safeguards to protect individual's privacy if such information is to be shared. Such entities should also clearly indicate to the person supplying the information any third party access to material supplied.

9.5.1.5 Effective Enforcement and Individual Remedies

In order to overcome the shortcomings associated with the self-regulation approach in regards to the lack of enforcement mechanism (detailed above), the PPL should assure individuals that they have the right to sue if their privacy has been violated. In case of remedies, the individuals have the right to seek a proper compensation for any actual damages, attorney and court fees, injunctive relief, and any other remedies that the court sees fit to protect individual privacy.

The proposed law should also grant individuals the right to sue for privacy violations in the international environment. This right may become difficult

to exercise by the individual concerned due to the obstacles created by conflict of jurisdiction. As a result, the question arises as to what individuals can do when their privacy rights have been violated in other countries. The second part of the proposed legal framework may provide a remedy to the aggrieved individuals in this context. The establishment of an independent governmental agency for privacy protection may assist the aggrieved parties to enforce their privacy rights both nationally and internationally. The following section examines the justification for and features of the proposed privacy agency.

9.5.2 The Jordanian Commission for Privacy Protection (JCPP)

In addition to the PPL, the proposed legal framework calls for the creation of the *Jordanian Commission for Privacy Protection (JCPP)*. This suggested name is based on the fact that, in recent times, the Government of Jordan has established many agencies to address issues and regulate activities of concerns to the Jordanian public.³⁴ It is possible to predict that, with the advancement of the ICT in Jordan, the issue of privacy will become a major concern to the general public. The establishment of an effective specialised privacy agency is required to address this concern. Further, the establishment of a privacy protection commission will put Jordan alongside the developed countries in regards to privacy protection. This may assist

³⁴ Since 1995, Jordan has established a number of governmental commissions which have full and separate power to the ministries. Examples of these commissions are: the Insurance Regulatory Commission (IRC), Public Transport Regulatory Commission (PTRC), Anticorruption Commission (AC), Civil Aviation Regulatory Commission (CARC), Electricity Regulatory Commission (ERC), Executive Privatisation Commission (EPC), Jordan Securities Commission (JSC), and the Telecommunications Regulatory Commission (TRC). Others include the Petra Region Commission (PRC), the Audiovisual Commission (AC), Coordination Commission for Social Solidarity (CCSS), Development Areas Commission (DAC), and the Jordanian Nuclear Energy Commission (JNEC). For information on these Commissions, see: <www.pm.gov.jo/english>.

Jordan, and particularly the private sector, to receive special treatment from these countries in relation to trade, political and technological support. The proposed JCPP should have the following features: regulatory authority and advisory role, independence, JCPP and the private sector, and educational and awareness role.

9.5.2.1 Regulatory Authority and Advisory Role

The proposed *Commission for Privacy Protection* (JCPP) would have regulatory powers and an advisory role. These features are based on a number of grounds. First, at the time of writing, such a Commission would be the first of its kind in Jordan with special task of protecting personal information — and not just in the context of ICT, as it would also include all activities in Jordan. It is necessary for the first Commission to have regulatory authority in order to enforce its own policies and guidelines. The Commission would also be responsible for the enforcement of the provisions of the PPL. This feature of regulatory authority is significant for the concept of privacy to be legally and socially evolved in the Jordanian society.

Secondly, the regulatory role granted to the Commission (JCPP) provides a flexible channel to address any legal shortcomings as a result of the application of the proposed PPL. Due to the rapid changes and development of the ICT, it is possible for any one law when it is drafted to anticipate accurately and accommodate the advancements that will emerge over time. As a result, the role of the Commission here is to provide regulations to address any privacy issues that may arise with the changes in ICT. In

anticipation of such developments and to reduce delays that might otherwise occur if an amendment were required for each and every technological advance, the Act that establishes the Commission will give it the appropriate powers to address issues up-to-date.

Thirdly, it has stated above that Jordan has a number of commissions that have regulatory authority to enforce different responsibilities and duties for different industries. However, none of these Commissions has the power to enforce privacy rights, nor the responsibility to provide privacy protection. It is not only possible but desirable to provide similar powers and the legal authority to enforce and oversight individual privacy rights in one independent national privacy Commission as it will bring the necessary expertise together and provide a single source of authority on the issue rather than have this dissipated through numerous industry commissions. It also has implications for implementation and enforcement (see below).

Fourthly, the proposed privacy Commission (JCPP) would have the role of investigating privacy violations committed by either governmental agency or private sectors against individuals, able to issue warning/s and/or imposing penalties on the violators. In order to protect individual privacy, it is required that the Commission (JCPP) have full investigative powers, and powers that would also include the ability to impose sanctions against relevant parties.

A number of other powers should also be considered for the proposed JCPP. It might also have the role of issuing advisory opinions and

recommendations to governmental agencies, private businesses and individuals; and be able to issue binding rules at the time of privacy disputes between these actors if they agreed that their disputes would be heard before the JCPP, that is, the JCPP could act as a mediation forum, enabling matters to be solved without costly court actions that might otherwise occur.

9.5.2.2 Independence

The second most important feature to the proposed JCPP would be its independence. The Commission should have the ability to criticise the policies and practices of the government towards privacy. It has been stated above that the Government of Jordan is one of the largest collectors of personal information. Therefore, the government practices should be subject for independent investigations by the proposed Commission.³⁵

Furthermore, the proposed Commission should also be independent when monitoring and criticising the private sector practices. For greater profit, some business industries may attempt to influence the way the Commission carries out its activities or on its decisions. For example, if the proposed Commission found that sending soliciting messages to customer after certain time of the day was an invasion of his/her privacy, the Commission may come under severe pressure from the telecommunications sector.

The guarantee of independence for the proposed Commission is significant in terms of Jordan's privacy approach meeting the adequacy requirement stated

³⁵ Robert Gellman, 'Enforcing Privacy Rights: Remediating Privacy Wrongs - New Models: A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board' (2003) 54 *Hasting Law Journal* 1183, 1208.

in the EU Directive. The EU Directive in recital 62 provides clearly that ‘complete independence’ is an ‘essential component’ of the protection of personal privacy.³⁶ For this, the EU Directive requires that each Member States have an independent supervisory authority with full power to investigate, to intervene, and to engage in legal proceedings.³⁷ In order for the proposed Commission to have this authority, the Commission must be an independent.

9.5.2.3 The JCPP-Private Sector Relationship

The proposed Commission should encourage the private sector to initiate and design privacy policies for the protection of personal information. A significant role that the proposed Commission can play in this context is to facilitate, develop and approve privacy standards created by the private sector. The relationship between the proposed Commission and the private sector should be cooperative rather than one of conflict. Both should have the same goal, which is the protection of individual privacy. This cooperative relationship would benefit individuals and businesses. The benefit for individuals is that they would be able to have more trust and confidence in private sectors’ policies that have been approved by an independent agency for privacy protection. The benefit for the businesses is the ability to create privacy policies suitable for their relevant industry with the approval and support of an independent agency responsible with protecting individual privacy. The outcome would be a greater trust in and greater credibility of

³⁶ *Directive 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 [1995] OJ L 8/1, 23 November 1995, recital 62.*

³⁷ *Ibid* art 28.

privacy regulations formulated down by the private sector and approved by the regulator.³⁸

9.5.2.4 Educational and Awareness Role

The proposed Commission would have the role to educate and increase awareness of privacy rights, choices and obligations within the society. For the Commission to deliver its privacy message, the establishment of communications channels with the general public is required. The Commission can achieve this through publications on the issue of privacy. These publications should be up-to-date, accurate, informative and easy to understand by a large number of people. In addition, the Commission should create its own Website.³⁹ Through this Website individuals would have greater access to relevant material and be able to read more about their privacy rights and make recommendations for policy change. Further, through the proposed Website individuals should be able to lodge formal complaints against any entity (public or private) if they believe that their privacy rights have been violated. Naturally such lodgement would be confidential.

³⁸ Gellman, above n 31, 1213.

³⁹ A possible portal of such website can be proposed as <<http://www.jcpp.gov.jo>>.

BIBLIOGRAPHY

The NOBLE QUR'AN: Translation of the Meanings of the Noble Qur'an in the English Language: by Dr Muhammad Taqi-ud-Din al-Hilali and Dr Muhammad Muhsin Khan (King Fahd Complex for the Printing of the HOLY QUR'AN)

The Meaning of the Holy Qur'an: Translated by Abdullah Yusuf Ali, Secretariat for Asia Assembly of Ulama (2005)

Commentary on the Riyad-us-Saliheen, Compiled by Al Imam Abu Zakariya Yahya bin Sharaf An-Nawawwi Ad-Dimashqi, Volume 1 (Darussalam, Riyadh, Saudi Arabia, 1999)

The Translation of the Meanings of Summarized Sahih Muslim: Arabic-English, Volume 2, Compiled by Al-Hafiz Zakiuddin Abdul-Azim Al-Mundhiri (Darussalam, Riyadh, Saudi Arabia, 2000)

Articles/ Books/ Journals

Agboola, Akinlolu and Oyesola Salawu, 'Optimizing the Use of Information and Communication Technology (ICT) in Nigerian Banks' (2008) 13(1) *Journal of Internet Banking and Commerce* 1

Akindemowo, Olujokè, *Information Technology Law in Australia* (1999)

Allen, Anita L, 'Minor Distractions: Children, Privacy and E-Commerce' (2001) 38 *Houston Law Review* 751

Allen, Anita L, *Uneasy Access: Privacy for Women in a Free Society* (1988)

Almatarneh, Akram, 'Privacy Implications for Information and Communications Technology (ICT): The Case of the Jordanian e-Government' in Sylvia M Kierkegaard (ed), *Private Law: Rights, Duties & Conflicts* (2010)

Anderton, Brian et al, 'The Impacts of Information Technology on the Financial Services Sector' in Brian Anderton (ed), *Current Issues in Financial Services* (1995)

Ang, Peng Hwa, 'The Role of Self-Regulation of Privacy and the Internet' (2001) 1(2) *Journal of Interactive Advertising* 76

An-Na'im, Abdullahi Ahmed, *Toward an Islamic Reformation: Civil Liberties, Human Rights, and International Law* (1990)

Arab Advisors Group, 'Jordan Internet users and e-commerce survey 2010' (Arab Advisors Group, 2010)

Assey, James M and Demetrios A Eleftheriou, 'The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?' (2001) 9 *CommLaw Conspectus* 145

Association of Banks in Jordan, *Association of Banks in Jordan 29th Annual Report 2007* (Association of Banks in Jordan, 2007)

Association of Banks in Jordan, 'Development of the Jordanian Banking Sector (2000-2009)' (Association of Banks in Jordan 2010)

Association of Banks in Jordan, 'Development of the Jordanian Banking Sector' (Association of Banks in Jordan, 2008)

Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* Report No 108 (2008)

Ayres, Ian and Matthew Funk, 'Marketing Privacy' (2003) 20 *Yale Journal on Regulation* 77

Azmi, Ida Madieha, 'Personal Data Protection Law: The Malaysian Experience' (2007) 16(2) *Information and Communications Technology Law* 125

Baderin, Mashood A, *International Human Rights and Islam* (2003)

Bannerman, Patrick, *Islam in Perspective: A Guide to Islamic Society, Politics and Law* (1988)

Basu, Subhajit, 'E-Government and Developing Countries: An Overview' (2004) 18(1) *International Review of Law Computers and Technology* 109

Batista, Paul J, 'The Perils of Telemarketing under the *Telephone Consumer Protection Act*: Sending Unsolicited Faxes Costs Dallas Cowboys \$1.73 Million, Leaves Dallas Mavericks under Full Court Pressure' (2003) 25 *Hastings Communications and Entertainment Law Journal* 231

Baumer, David L, Julia B Earp and J.C. Poindexter, 'Internet Privacy Law: A Comparison between the United States and the European Union' (2004) 23 *Computers and Security* 400

Baylouny, Anne Marie, 'Militarizing Welfare: Neo-liberalism and Jordanian Policy' (2008) 62(2) *Middle East Journal* 277

Belanger, France Belanger and Janine S Hiller, 'A Framework for E-Government: Privacy Implications' (2006) 12(1) *Business Process Management Journal* 48

Bennett, Colin J and Charles D Raab, 'The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response' (1997) 13 *The Information Society* 245

Boyd, Virginia, 'Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization' (2006) 24(3) *Berkeley Journal of International Law* 939

Braizat, Fares 'Democracy in Jordan 2007' (Centre for Strategic Studies-University of Jordan, 2007)

Bressie, Kent, Michael Kende and Howard Williams, 'Telecommunications trade liberalisation and the WTO' (2005) 7(2) *Info* 3

Budnitz, Mark E, 'Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate' (1998) 49 *South Carolina Law Review* 847

Business Monitor International, 'Jordan Telecommunications Report Q2 2009: Including 5-year industry forecasts' (2009)

Business Monitor International, 'Jordan Telecommunications Report Q3 2008: Including 5-year industry forecasts' (2008)

Business Monitor International, 'Jordan Telecommunications Report Q4 2008: Including 5-year industry forecasts' (2008)

Buss, Martin D J, 'Legislative Threat to Transborder Data Flow' (1984) 62(3) *Harvard Business Review* 111

Bygrave, Lee A, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6(3) *International Journal of Law and Information Technology* 247

Camden, Bonnie G 'Fair Credit Reporting Act: What You Don't Know May Hurt You' (1988) 57 *Cincinnati Law Review* 267

Campbell, Angela J, 'Self-Regulation and the Media' (1999) 51 *Federal Communications Law Journal* 711

Caral, Jose M A Emmanuel A, 'Lessons from ICANN: Is Self-Regulation of the Internet Fundamentally Flawed?' (2004) 12(1) *International Journal of Law and Information Technology* 1

Cassing, James and Anna Maria Salameh, 'Jordan - United States Free Trade Agreement Economic Impact Study: Searching for Effects of the FTA on Exports, Imports and Trade Related Investments' Final Report (United States Agency for International Development (USAID), 2006)

Cate, Fred H, *Privacy in the Information Age* (1997)

Cate, Fred H, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer Protection in the Age of the Information Economy* (2006) 341

Caudill, Eve M and Patrick E Murphy, 'Consumer Online Privacy: Legal and Ethical Issues' (2000) 19(1) *Journal of Public Policy and Marketing* 7

Cavoukian, Ann and Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (1997)

Cavoukian, Ann, 'The Promise of Privacy-Enhancing Technologies: Applications in Health Information Networks' in Colin J Bennett and Rebecca Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (1999) 116

Chuan Sun, 'The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective' (2003) 2(1) *Northwestern Journal of Technology and Intellectual Property* 99

Ciborra, Claudio and Diego D Navarra, 'Good Governance, Development Theory, and Aid Policy: Risks and Challenges of E-Government in Jordan' (2005) 11(2) *Information Technology for Development* 141

Ciborra, Claudio, 'Interpreting E-Government and Development: Efficiency, Transparency or Governance at a Distance?' (2005) 18(3) *Information Technology and People* 260

Cody, Jonathan P, 'Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation' (1999) 48 *Catholic University Law Review* 1183

Coleman, Allison, *The Legal Protection of Trade Secrets* (1992)

Commission of the European Communities, 'Implementation of the European Neighbourhood Policy in 2008: Progress Report Jordan' (2009)

Cook, Catriona et al, *Laying Down the Law* (5th ed, 2001)

Cooper, Henry M, 'The *Electronic Communications Privacy Act*: Does the Answer to the Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis' (2001) 20 *John Marshall Journal of Computer and Information Law* 1

Creane, Susan et al, 'Financial Sector Development in the Middle East and North Africa' IMF Working Paper No 04/201 (International Monetary Fund, 2004)

Cuaresma, Jolina C, 'V. Business Law: B. Privacy: 1. Financial Services: The Gramm-Leach-Bliley Act' (2002) 17 *Berkeley Technology Law Journal* 497

Cunningham, Karla J Cunningham, 'Factors Influencing Jordan's Information Revolution: Implications for Democracy' (2002) 56(2) *Middle East Journal* 240

- Davies, Simon and Ian Hosein, 'Liberty on the Line' in Liberty (National Council for Civil Liberties) (ed), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (1999) 68
- Debusseré, Frederic, 'The EU-E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?' (2005) 13(1) *International Journal of Law and Information Technology* 70
- DeCew, Judith Wagner, 'The Scope of Privacy in Law and Ethics' (1986) 5(2) *Law and Philosophy* 145
- Dempsey, James X, 'Communications Privacy in the Digital Age: Revitalising the Federal Wiretap Laws to Enhance Privacy' (1997) 8 *Albany Law Journal of Science and Technology* 65
- Dempsey, James X, Paige Anderson and Ari Schwartz, 'Privacy and E-Government: A Report to the United Nations Department of Economic and Social Affairs as background for the *World Public Sector Report: E-Government*' (Center for Democracy and Technology, 2003)
- Department of Economic and Social Affairs, 'Global E-Government Readiness Report 2005: From E-Government to E-Inclusion' (United Nations, 2005)
- Department of Economic and Social Affairs, 'United Nations E-Government Survey 2008: from E-Government to Connected Governance' (United Nations, 2008)
- Dorney, Maureen S, 'Privacy and the Internet' (1997) 19 *Hastings Communications and Entertainment Law Journal* 635
- Doyle, Carolyn and Mirko Bagaric, *Privacy Law in Australia* (2005)
- Edwards, George E, 'International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy' (2001) 26 *Yale Journal of International Law* 323
- Elsheikh, Yousef, Andrea Cullen and Dave Hobbs, 'E-Government in Jordan: Challenges and Opportunities' (2008) 2(2) *Transforming Government: People, Process and Policy* 83
- Erbschloe, Michael and John Vacca, *Net Privacy: A Guide to Developing and Implementing an Ironclad E-Business Privacy Plan* (2001)
- Ergene, Bogac A, *Judicial Practice: Institutions and Agents in the Islamic World* (2009)
- European Parliament, 'Report on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles (C5-0280/2000-2000/2144 (COS)' (RR\285929EN.doc, 2000)

avail at: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/0117-02_en.pdf

Federal Trade Commission, 'Biennial Report to Congress: Pursuant to the *Do Not Call Registry Fee Extension Act of 2007*' (2009)

Federal Trade Commission, 'Privacy of Consumer Financial Information: 16 CFR Part 313' (2000) 65(101) *Federal Register* 33646

Fensterstock, Blair C, 'The Public and the Fair Reporting Act' in Theodore R Kupferman (ed), *Privacy and Publicity* (1990)

Flaherty, David H, *Protecting Privacy in Surveillance Societies* (1989)

Foord, Kate, 'Defining Privacy' Occasional Paper (Victorian Law Reform Commission, 2002)

Foster, Scott, 'Online Profiling is on the Rise: How Long until the United States and the European Union Lose Patience with Self-Regulation' (2000) 41 *Santa Clara Law Review* 255

Fried, Charles, 'Privacy' (1968) 77 *Yale Law Journal* 475

Fromholz, Julia M, 'Data Privacy: The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 461

Gavison, Ruth, 'Privacy and the Limits of Law' (1980) 89(3) *Yale Law Journal* 421

Gellman, Robert Gellman, 'Enforcing Privacy Rights: Remedying Privacy Wrongs – New Models: A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board' (2003) 54 *Hastings Law Journal* 1183

George, Barbara Crutchfield, Patricia Lynch and Susan J Marsnik, 'U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive' (2001) 38 *American Business Law Journal* 735

Ghosh, Anup K, *Security and Privacy for E-Business* (2001)

Gladstone, Julia, 'The Impact of E-Commerce on the Laws of Nations: The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy' (2000) 7 *Willamette Journal of International Law and Dispute Resolution* 10

Glancy, Dorothy J, 'The Invention of the Privacy' (1979) 21(1) *Arizona Law Review* 1

- Glenn, Catherine Louisa, 'Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records' (2000) 53 *Vanderbilt Law Review* 1605
- Gomez, Joshua, Travis Pinnick and Ashkan Soltani, 'Know Privacy' (UC Berkeley, School of Information, 2009)
- Gottlieb, Calvin, 'Privacy: A Concept Whose Time Has Come and Gone' in David Lyon and Elia Zureik (eds), *Computers, Surveillance, and Privacy* (1996) 156
- Government of Jordan, 'Statement of Government Policy 2007 on the Information & Communications Technology & Postal Sectors' (Ministry of Information & Communications Technology, 2007)
- Graham, Jonathan P, 'Privacy, Computers and the Commercial Dissemination of Personal Information' (1986) 65 *Texas Law Review* 1395
- Greenleaf, Graham Greenleaf, 'Asia- Pacific Developments in Information Privacy Law and its Interpretation' (2007) 5
- Greenleaf, Graham, 'The 1995 EU Data Protection Directive on Data Protection: An Overview' (1995) 3(2) *International Privacy Bulletin* 1
- Greenwood, Scott, 'Jordan's "New Bargain": The Political Economy of Regime Security' (2003) 57(2) *Middle East Journal* 248
- Gross Hyman, 'Privacy and Autonomy' in Roland Pennock and John W Chapman (eds), *Privacy* (1971)
- Gross, Hyman 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34
- Gutwirth, Serge Gutwirth, *Privacy and the Information Age* (2002)
- Halewood, Naomi and Charles Kenny, 'Young People and ICTs in Developing Countries' (2008) 14(2) *Information Technology for Development* 171
- Hashemi, Kamran, *Religious Legal Traditions, International Human Rights Law and Muslim States* (2008)
- Hatch, Mike, 'The Privatization of Big Brother: Protecting Sensitive Personal Information From Commercial Interests in the 21st Century' (2001) 27 *William Mitchell Law Review* 1457
- Hayat, Muhammad Aslam, 'Privacy and Islam: From the Quran to Data Protection in Pakistan' (2007) 16(2) *Information and Communications Technology Law* 137

- Henderson, Harry, *Privacy in the Information Age* (1999)
- Hendi, Ala'eddin Kanza'l-Ummâl fi Sunan wa'l-Aqwal wa-'l-Afal, Vol 3/808 Hadith; 8827
- Hietala, Jim, 'Managing Information Privacy' (2008) 21(3) *Bank Accounting and Finance* 41
- Hijazi, Emad Hamdy, *Al haq fel Khososya wa Masooliyat Al sahafy: Fe Doo2 Ahkam Alsharee'a Aleslamyha wal Alganoon Almadany* (2008)
- Holtzman, David H, *Privacy Lost: How Technology Is Endangering Your Privacy* (2006)
- Human Rights Committee, *Consideration of Reports Submitted by States parties under Article 40 of the Covenant: Fourth Periodic Report of Jordan* (CCPR/C/JOR/4; CCPR/C/JOR/Q/4 and Add.1HRI/CORE/1Add.18/Rev.1): 100th sess, sum record of 2748th mtg, 13 October 2010 CCPR/C/SR.2748
- Husain, Sheikh Showkat, 'Human Rights in Islam Principles and Precedents' in Tahir Mahmood (ed), *Human Rights in Islamic Law* (1993)
- Hussain, Jamila, *Islam: Its Law and Society* (2nd ed, 2004)
- Information Technology Association Jordan (int@j), 'Jordan's Information Society a Fast Growing Sector for a Transforming Nation' (Economic and Social Commission for Western Asia, 2003)
- Information Technology Association-Jordan (int@j), 'ICT & ITES Industry Statistics & Yearbook' (Information Technology Association-Jordan (int@j), 2009) avail: http://www.intaj.net/sites/default/files/2009_ICT__ITES_Industry_Statistics__Yearbook_Final.pdf
- Iqbal, Zafar and Mervyn K. Lewis, *An Islamic Perspective on Governance* (2009)
- Jamtgaard, Laurel, 'Big Bird Meets Big Brother: A Look at the *Children's Online Privacy Protection Act*' (2000) 16 *Computer High Technology Law Journal* 385
- Janger, Edward J and Paul M Schwartz, 'The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules' (2001) 86 *Minnesota Law Review* 1219
- Joeson Wong Ka Yu, 'Electronic Government and its Implication for Data Privacy in Hong Kong: Can Personal Data (Privacy) Ordinance Protect the Privacy of Personal Information in Cyberspace?' (2005) 19(2) *International Review of Law Computers and Technology* 143

- Jordan Investment Board, *Annual Report* (Jordan Investment Board, 2006)
- Kamali, Mohammad Hashim, *The Right to Life, Security, Privacy and Ownership in Islam* (2008)
- Khatab, Sayed and Gary D Bouma, *Democracy in Islam* (2007)
- Kizza, Joseph Migga, 'Anonymity, Security, Privacy and Civil Liberties' in David Gries and Fred B Schneider (eds), *Ethical and Social Issues in the Information Age* (3rd ed, 2007)
- Kleiman, Matthew N, 'The Right to Financial Privacy versus Computerized Law Enforcement: A New Fight in an Old Battle' (1992) 86 *Northwestern University Law Review* 1169
- Klosek, Jacqueline Klosek, *Data Privacy in the Information Age* (2000)
- Kritzer, Herbert M (ed), *Legal Systems of the World: A Political, Social and Cultural Encyclopedia* (2002)
- Kronman, Anthony T, 'The Privacy Exemption to the Freedom of Information Act' (1980) 9 *Journal of Legal Studies* 727
- Kuanpoth, Jakkrit, 'Harmonisation of TRIP-Plus IPR Policies and Potential Impacts on Technological Capability: A case study of the pharmaceutical industry in Thailand' (International Centre for Trade and Sustainable Developments (ICTSD), 2006)
- Law Reform Commission of New Zealand, 'Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy. Stage 3' Report No 113 (Law Commission of New Zealand, 2009)
- Leathers, Daniel R Leathers, 'Giving Bite to the EU-U.S. Data Privacy Safe Harbour: Model Solutions for Effective Enforcement' (2009) 41 *Case Western Reserve Journal of International Law* 193
- Lee, Kelley, *Global Telecommunications Regulation: A Political Economy Perspective* (1996)
- Lee, Ya-Ching Lee, 'Will Self-Regulation Work in Protecting Online Privacy?' (2003) 27(4) *Online Information Review* 276
- Lindsay, David, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131
- Lobell, Steven E, 'The Second Face of American Security: The US-Jordan Free Trade Agreement as Security Policy' (2008) 27 *Comparative Strategy* 88

- Loewe, Markus Loewe, Jonas Blume and Johanna Speer, 'How Favoritism Affects the Business Climate: Empirical Evidence from Jordan' (2008) 62(2) *Middle East Journal* 259
- Long, William J and Mark Pang Quek, 'Personal Data Privacy Protection in an Age of Globalisation: the US-EU Safe Harbour Compromise' (2002) 9(3) *Journal of European Public Policy* 325
- Malkawi, Bashar H, 'E-Commerce in Light of International Trade Agreements: The WTO and the United States-Jordan Free Trade Agreement' (2006) 10 *International Journal of Law and Information Technology* 1
- Marsh, Richard M Jr, 'Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Information on the Internet' (2009) 15 *Michigan Telecommunications and Technology Law Review* 543
- Masur, Steven, 'Mobile Phone Text Message Spam: Building a Vibrant Market for Mobile Advertising while Keeping Customers Happy' (2007) 7 *Virginia Sports and Entertainment Law Journal* 41
- Maxwell, Kimera and Roger Reinsch, 'The Freedom of Information Act Privacy Exemption: Who Does It Really Protect?' in Theodore R Kupferman (ed), *Privacy and Publicity* (1990)
- McDonagh, Maeve, 'E-Government in Australia: the Challenge to Privacy of Personal Information' (2002) 10(3) *International Journal of Law and Information Technology* 327
- McLean, Deckle McLean, *Privacy and Its Invasion* (1984)
- McNamara, Kerry S, 'Information and Communication Technologies, Poverty and Development: Learning from Experience' Background Paper for the infoDev Annual Symposium, 9-10 December 2003, Geneva, Switzerland (The World Bank, 2003)
- Merkow, Mark S and James Breithaupt, *The E-Privacy Imperative: Protect Your Customers' Internet Privacy and Ensure Your Company's Survival in the Electronic Age* (2002)
- Michael, James, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994)
- Miller, Arthur Raphael, *The Assault on Privacy: Computers, Data Banks and Dossiers* (1971)
- Miller, Roger LeRoy and Gaylord A Jentz, *Fundamentals of Business Law: Excerpted Cases* (2nd ed, 2010)

Ministry of Industry and Trade 'Research & Development Strategy for Information and Communication Technology 2007-2010' (2007)

Ministry of Industry and Trade, 'Assessment of Trade in Services of the Hashemite Kingdom of Jordan: A Project of the Ministry of Industry and Trade (MoIT) and United Nation Conference on Trade and Development (UNCTAD)' (2006) Part II, avail <http://www.mit.gov.jo/portals/0/the%20study%20-%20all%20parts.pdf>

Ministry of Information and Communications Technology (MoICT), 'National ICT Strategy of Jordan 2007-2011' (Ministry of Information and Communications Technology, 2007)

Monahan, Amy, 'Deconstructing Information Walls: The Impact of the European Data Directive on US Businesses' (1998) 29 *Law and Policy in International Business* 275

Moore, Dudley J, *Privacy: The Press and the Law* (2003)

Moore, Roy L, 'The 1978 *Right to Financial Privacy Act* and U.S. Banking Law' in Theodore R Kupferman (ed), *Privacy and Publicity* (1990)

Morales-Gomez, Daniel and Martha Melesse, 'Utilising Information and Communication Technologies for Development: The Social Dimensions' (1998) 8(1) *Information Technology for Development* 3

Mulligan, Deidre K and Janlori Goldman, 'The Limits and the Necessity of Self-Regulation: The Case for Both' in *Privacy and Self-Regulation in the Information Age* (US Department of Commerce, 1997)

Murray, Patrick J, 'The Adequacy Standard under Directive 95/46/EC: Does U.S. Data Protection Meet this Standard?' (1998) 21 *Fordham International Law Journal* 932

Myers, Jennifer M, 'Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States' (1997) 29 *Case Western Reserve Journal of International Law* 109

Nabulsi, Mohammad, 'Implementation of Jordan-EU Action Plan: A CSS Independent Evaluation' (Centre for Strategic Studies, University of Jordan, 2009)

National Centre for Human Rights, 'State of Human Rights in the Hashemite Kingdom of Jordan (2008)' (National Centre for Human Rights, 2008)

New Zealand Law Commission, 'Privacy: Concepts and Issues: Review of the Law of Privacy. Stage 1' Study Paper No 19 (2008)

New Zealand Law Reform Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (Government of New Zealand, 2008)

Newman, Simon and Gavin Sutter, 'Electronic Payments – The Smart Card: Smart Cards, E-Payments & Law- Part I' (2002) 18(4) *Computer Law and Security Report* 235

Nowak, Manfred, 'Civil and Political Rights' in Janusz Symonides (ed), *Human Rights: Concept and Standards* (2000)

Organisation for Economic Co-operation and Development (OECD), *The E-Government Imperative* (2003)

Pandozzi, Neal R Pandozzi, 'Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation' (2001) 55 *University of Miami Law Review* 163

Parker, Richard B, 'A Definition of Privacy' (1974) 27(2) *Rutgers Law Review* 275

Pattison, Patricia and Anthony F McGann, 'General Law Division: State Telemarketing Legislation: A Whole Lotta Law Goin' on!' (2003) 3 *Wyoming Law Review* 167

Petersen, Sandra Byrd, 'Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?' (1995) 48 *Federal Communications Law Journal* 163

Post, Robert, 'Three Concepts of Privacy' (2001) 89(6) *Georgetown Law Review* 2087

Prosser, William L, 'Privacy' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984)

Quirk, Patrick, 'Privacy Laws and Policy' in Patrick Quirk and Jay Forder (eds), *Electronic Commerce and the Law* (2nd ed, 2003) 332

Rachels, James, 'Why Privacy is Important' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 290

Ratish, Robert, 'Democracy's Backlog: The *Electronic Freedom of Information Act* Ten Years Later' (2007) 34 *Rutgers Computer and Technology Law Journal* 211

Redden, Kenneth Robert , 'The Legal System of Jordan', in Kenneth Robert Redden (ed), *Modern Legal Systems Cyclopedia* (1990)

Regan, Pricilla M, 'Safe Harbours or Free Frontiers? Privacy and Transborder Data Flows' (2003) 59(2) *Journal of Social Issues* 263.

Regan, Priscilla M, 'The Globalization of Privacy: Implications of Recent Changes in Europe' (1993) 52(3) *American Journal of Economics and Sociology* 257

Regan, Priscilla M, *Legislating Privacy: Technology, Social Values and Public Policy* (1995)

Regan, Priscilla M, 'Privacy in an Electronic Government Context' in Hsinchun Chen et al (eds), *Digital Government: E-Government Research, Case Studies, and Implementation* (2008)

Regan, Priscilla M, 'The United States' in James B Rule and Graham Greenleaf (eds), *Global Privacy Protection: the First Generation* (2008)

Reiman, Jeffrey H, 'Privacy, Intimacy and Personhood' (1976) 6 *Philosophy and Public Affairs* 26

Reynolds, George W, *Ethics in Information Technology* (2nd ed, 2007)

Rita Marie Cain, 'Global Privacy Concerns and Regulation – Is the United States a World Apart?' (2002) 16(1) *International Review of Law Computers and Technology* 23

Rotenberg, Marc, 'Modern Studies in Privacy Law: Privacy and Secrecy after September 11' (2002) 86 *Minnesota Law Review* 1115

Rule, James and Lawrence Hunter, 'Towards Property Rights in Personal Data' in Colin J Bennett and Rebecca Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (1999)

Rustud, Michael L and Cyrus Daftary, *E-Business Legal Handbook* (2002)

Salbur, Steven R, 'The European Union Data Privacy Directive and International Relations' (2002) 35 *Vanderbilt Journal of Transnational Law* 655

Samuelson, Pamela, 'Book Review: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy' (1999) 87 *California Law Review* 751

Schaechter, Andrea, 'Issues in Electronic Banking: An Overview' (International Monetary Fund, 2002)

Schoeman, Ferdinand, 'Privacy and Intimate Information' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984)

Schwartz, Paul M and Joel R Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996)

- Schwartz, Paul M, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 *Iowa Law Review* 471
- Schwartz, Paul M, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1994) 80 *Iowa Law Review* 553
- Senturk, Recep, 'Sociology of Rights' in Abdul Aziz Said, Mohammed Abu-Nimer and Meena Sharify-Funk (eds), *Contemporary Islam: Dynamic, Not Static* (2006)
- Sessler, Joshua B, 'Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet' (1996) 5 *Journal of Law and Policy* 627
- Shaffer, Gregory C, 'Globalisation and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards' (2000) 25 *Yale Journal International Law* 1
- Shalhoub, Zeinab Karake Shalhoub, 'Trust, Privacy, and Security in Electronic Commerce Business: The Case of the GCC Countries' (2006) 14(3) *Information Management and Computer Security* 270
- Smith, Robert Ellis, *Privacy* (1979)
- Solove, Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (3rd ed, 2009)
- Solove, Daniel J, 'Access and Aggregation: Public Records, Privacy and the Constitution' (2001) 86 *Minnesota Law Review* 1137
- Solove, Daniel J, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087
- Solove, Daniel J, *The Digital Person: Technology and Privacy in the Information Age* (2004)
- Solove, Daniel J, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (2007)
- Sparks, Shaun A, 'The Direct Marketing Model and Virtual Identity: Why the United States should Not Create Legislative Controls on the Use of Online Consumer Personal Data' (2000) 18 *Dickinson Journal International Law* 517
- Staples, William G (ed), *Encyclopedia of Privacy* (2007)
- Svantesson, Dan Jerker B, 'Protecting Privacy on the 'Borderless' Internet- Some thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168

- Svantesson, Dan Jerker B, 'The right of reputation in the Internet era' (2009) 23(3) *International Review of Law Computers & Technology* 169
- Sweet, James, 'Opting-Out of Commercial Telemarketing: The Constitutionality of the National Do-Not-Call Registry' (2003) 70 *Tennessee Law Review* 921
- Swire, Peter P and Robert E Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998)
- Swire, Peter P, 'Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information' in 'Privacy and Self-Regulation in the Information Age' (US Department of Commerce, 1997)
- Swire, Peter P, 'The Surprising Virtues of the New Financial Privacy Law' (2001) 88 *Minnesota Law Review* 1263
- Tallman, David A, 'Financial Institution and the Safe Harbor Agreement: Securing Cross-Border Financial Data Flows' (2003) 34 *Law and Policy in International Business* 747
- Tavani, Herman T, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology* (2nd ed, 2007)
- Telecommunications Regulatory Commission (Jordan), *Annual Report 2007* (2007)
- Telecommunications Regulatory Commission (TRC), 'Annual report 2009' (Telecommunications Regulatory Commission (TRC), 2009) 65, Appendix (3) avail: www.trc.gov.jo
- Thompson, Suzanne M, 'The Digital Explosion Comes With a Cost: the Loss of Privacy' (1999) 4 *Journal of Technology Law and Policy* 3
- Thomson, Judith Jarvis, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295
- Tucker, Greg, *Information Privacy Law in Australia* (1992)
- Tyree, Alan and Andrea Beatty, *The Law of Payments Systems* (2000)
- Tyree, Alan and Prudence Weaver, *Weerasooria's Banking Law and the Financial System in Australia* (6th ed, 2006)
- Tyree, Alan L, *Digital Cash* (1997)
- United States Government Accountability Office, 'Privacy: Key Challenges Facing Federal Agencies' Testimony: Before the Subcommittee on Commercial and Administrative Law, Committee on the judiciary, House of Representatives –Statement of Linda D Koontz, Director, Information

Management Issues (United States Government Accountability Office, 2006)

US Department of Commerce, *US-EU Safe Harbour Framework: A Guide to Self-Certification* (2009)

Von Tigerstrom, Barbara, 'Protection of Health Information Privacy: The Challenges and Possibilities of Technology' (1998) 4 *Review of Current Law and Law Reform* 44

Wakana, Joann M, 'The Future of Online Privacy: A Proposal for International Legislation' (2003) 26 *Loyola of Los Angeles International and Comparative Law Review* 151

Waldo, James, Herbert S Lin and Lynette I Millett (eds), *Engaging Privacy and Information Technology in a Digital Age* (2007)

Walker, Kent, 'The Cost of Privacy' (2001) 25 *Harvard Journal of Law and Public Policy* 87

Warner, Janice and Soon Ae Chun, 'Privacy Protection in Government Mashups' (2009) 14(1/2) *Information Polity* 75

Warren, Samuel D and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193

Weeramantry, C G, 'Islam and Human Rights' in Tahir Mahmood (ed), *Human Rights in Islamic Law* (1993)

Westin, Alan F, 'Science, Privacy and Freedom: Issues and Proposals for the 1970s: Part 1 – The Current Impact of Surveillance on Privacy' (1966) 66 *Columbia Law Review* 1003

Westin, Alan F, *Privacy and Freedom* (1967)

White, Alison, 'Control of Transborder Data Flow: Reactions to the European Data Protection Directive' (1997) 5(2) *International Journal of Law and Information Technology* 230

Wilson, Ernest J III, *The Information Revolution and Developing Countries* (2004)

World Economic Forum, 'The Global Information Technology Report 2009-1010: ICT for Sustainability' (The World Economic Forum, 2009)

World Trade Organisation, 'Report of the Working Party on the Accession of the Hashemite Kingdom of Jordan to the World Trade Organisation' (1999)

<http://docsonline.wto.org/DDFDdocuments/t/WT/ACC/JOR33.DOC>

World Trade Organisation, 'Report of the Working Party on the Accession of Jordan to the World Trade Organisation: Trade in Services: Schedule of Specific Commitments on Services' (World Trade Organisation, 1999) 14-15, Report No WT.ACC/JOR/33/Add.2, avail http://www.mit.gov.jo/Portals/0/wot/services_schedule.pdf.

World Trade Organization, 'Trade Policy Review of Jordan: Report by the Secretariat' (World Trade Organization, 2008)

Zaidi, Kamaal, 'Harmonizing U.S- EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data' (2003) 12 *Michigan State Journal of International Law* 169

Zakaria, Norhayati, Jeffrey M Stanton and Shreya T M Sarkar-Barney, 'Designing and Implementing Culturally-Sensitive IT Applications: The Interaction of Culture Values and Privacy Issues in the Middle East' (2003) 16(1) *Information Technology and People* 49

Zwick, Detlev and Nihilesh Dholakia, 'Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right' (2001) 11(2) *Electronic Markets* 116

CASES

Ali v Playgirl Inc, 447 F Supp 723 (SDNY 1978)

Andrew v Veterans Administration, 838 F 2d 418, 425 (10th Cir, 1988)

Arrington v New York Times, 434 NE 2d (NY Ct. App 1982)

B v France (1992) 16 EHRR 1

Barber v Time, Inc., 159 SW 2d 291 (Mo 1942)

Burghartz v Switzerland (1994) 18 EHRR 101

California Bankers Association v Shultz, 416 US 21 (1974)

Carson v Here's Johnny Portable Toilets Inc, 698, F 2d 831 (6th Cir, 1983)

Central Hudson Gas and Electric Corp v. Public Service Commission, 447 US 557, 561 (1981)

Daily Times Democrat v Graham, 162 So 2d 474 (Ala 1964)

Department of the Air Force v Rose, 425 US 352 (1976)

Destination Ventures Ltd v Federal Communications Commission, 46 F 3d 54 (9th Cir, 1995)

Dudgeon v United Kingdom (1982) 4 EHRR 149

Dun & Bradstreet, Inc v Greenmoss Builders, Inc 472 US 749 (1985)
Federal Trade Commission (FTC) v GeoCities, File No 982 3015, Docket No C-3850

Federal Trade Commission (FTC) v Toysmart.com, LLC, and Toysmart.com Inc, Civil Action No 00-11341-RGS, FTC File No X000075

Friedl v Austria (1996) 21 EHRR 83

Griswold v Connecticut, 381 US 479 (1965)

Hendry v Connor, 303 Minn 317, 226 NW 2d 921 (1975) 923

Hirsch v SC Johnson & Son Inc, 280 NW 2d 129 (Wis, 1979)

Huvig v France 11105/84 (1990) Eur Court HR, A176-B, (24 April 1990)

Katz v United States, 389 US 347 (1967)

McIntyre v Ohio Election Comm'n, 514 US 334 (1995)

Midler v Ford Motor Co, 849 F 2d 460 (9th Cir, 1988)

Moser v FCC, 46 F 3d 970, 971 (9th Cir, 1995)

Ms X and Y v Argentina, Inter-American Commission on Human Rights, Report No 38/96, Case No 10.506, Argentina, 15 October 1996, avail <<http://www.cidh.org>> at 12 December 2008

NAACP v Alabama, 357 US 449 462 (1958)

Niemietz v Germany 13710/88 (1992) Eur Court HR, A251-B (16 December 1992)

Olmstead v US 277 US 438 (1928)

Onassis v Christian Dior, 472 NYC 2d 254 (NY Supp, 1984)

Peck v United Kingdom (2003) 36 EHRR 41

Pretty v United Kingdom (2002) 35 EHRR 1

Productions Inc v Day & Night Co, 523 F Supp. 485 (SDNY 1981)

Talley v California, 362 US 60 (1960)

Thompson v Close-up Inc., 98 NYS 2D 300 (1950)

United States Department of Justice v Reporters Committee for Freedom of the Press, 489 US 749 (1989)

United States v Miller, 425 US 436 (1976)

United States v White, 401 US 745 (1971)

LEGISLATION

American Law Institute, *Restatement of the Law (Second) Torts* (1977) § 652

American Law Institute, *Restatement of the Law (Second) Torts* (1977) § 581

American Law Institute, *Restatement of the Law (Second) Torts* (1977) § 578

Anti-Corruption Commission Law No 62 of 2006, (Jordan) [Arabic] *Official Gazette No 4794*, on 30 November 2006, at 4534

Anti-Money Laundering Law No 46 of 2007, (Jordan) [Arabic] *Official Gazette No 4831*, 17 June 2007, at 4130

Bank Secrecy Act of 1970, 31 USC § 1951

Banking Law No 28 of 2000, (Jordan) *Official Gazette No 4448*, 1 August 2000, at 2950

Bill of Rights (Amendments 1-10 of the *Constitution of the United States of America*) National Archives of the United States of America <http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html>

Central Bank of Jordan Law No 23 of 1971, (Jordan) *Official Gazette No 2301*, on 25 May 1971

Children's Online Privacy Protection Act of 1998, 15 USC § 6501

Children's Online Privacy Protection Rule, 16 CFR § 312

Civil Law No 43 of 1976, (Jordan) [Arabic] *Official Gazette No 2645*, on 1 August 1976

Civil Courts Establishment Law No 17 of 2001, (Jordan) [Arabic] *Official Gazette No 4480*, on 18 March 2001, at 1308

Civil Procedure Code No 42 of 1952, (Jordan) [Arabic] *Official Gazette No 1113*, 16 June 1952, at 288.

Code of Criminal Procedure No 9 of 1961, (Jordan) [Arabic] *Official Gazette No 1539*, on 1 January 1961, at 311

Computer Matching and Privacy Protection Act of 1988, 5 USC § 552a

Constitution of the Hashemite Kingdom of Jordan, 8 January 1952 (Jordan)

Constitution of the United States of America, National Archives of the Government of the United States of America
<http://www.archives.gov/exhibits/charters/constitution_transcript.html>

Court of Serious Crimes Law No 19 of 1986, (Jordan) [Arabic] *Official Gazette No 3380*, 16 March 1986, at 457

Credit Information Law No 15 of 2010, (Jordan) [Arabic] *Official Gazette No 5034*, 1 June 2003, at 3071

Directive 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 [1995] OJ L 8/1

E-Government Act of 2002, 44 USC § 101

Electronic Communications Privacy Act of 1986, 18 USC § 2510

Electronic Freedom of Information Act Amendments of 1996, 5 USC § 552

Electronic Transaction Law No 85 of 2001, (Jordan) *Official Gazette, No 4524*, 31 December 2001, at 6010

Fair and Accurate Credit Transactions Act of 2003, 15 USC § 1601

Fair Credit Reporting Act, 15 USC § 1681

Family Protection Law No 6 of 2008, (Jordan) [Arabic] *Official Gazette No 4892*, 16 March 2008, at 821

Federal Trade Commission Act, 15 USC §§ 41- 58

Federal Trade Commission, *The Children's Online Privacy Protection Rule*, 16 CFR Part 312 (2000) Federal Trade Commission
<http://www.ftc.gov/privacy/privacyinitiatives/childrens_lr.html> at 04 February 2010

Freedom of Information Act, 5 USC § 552

Gramm-Leach-Bliley Act of 1999, 15 USC §§ 6801-6809

High Court of Justice No 12 of 1992, (Jordan) [Arabic] *Official Gazette No 3813*, 25 March 1992, at 516

Information Systems Crime Law No 30 of 2010, (Jordan) [Arabic] Official Gazette, No 5056, 16 September 2010, at 5334

Instruction for Regulating the Work of the Internet Centers and Cafés and the Bases for their Licensing for the year 2001 <http://www.reach.com.jo/Downloads/Legislative/Internet_Cafes_Regulations.pdf> at 26 November 2010

Investment Promotion Law No 16 of 1995 (Jordan)

Jordanian National Charter, December 1990 (Jordan)

Law on Guaranteeing the Right of Access to Information No 47 of 2007, (Jordan) [Arabic] Official Gazette No 4831, on 17 June 2007, at 4142

Magistrate Courts Law No 15 of 1952, (Jordan) [Arabic] Official Gazette No 1102, on 1 January 1952

Municipal Courts Establishment Law No 72 of 2001, (Jordan) [Arabic] Official Gazette No 4520, 2 December 2001, at 5567

National Centre for Human Rights Law No 51 of 2006, Official Gazette, 16 October 2006, at 4026 (Jordan) avail: <<http://www.nchr.org.jo>>

Panel Code No 16 of 1960, (Jordan) [Arabic] Official Gazette No 1487, on 1 January 1960

Payment System Regulations: Asool Gwaed Al Aamal wal Taleemat Al khasa Bel Magasa Al Electroonyh (Jordan) [Arabic]

Postal Services Law No 34 of 2007, (Jordan) [Arabic] Official Gazette No 4823, on 1 May 2007, at 2645

Privacy Act of 1974, 5 USC § 552a

Privatization Law No 25 of 2000 (Jordan).

Regulations of Anti-Money Laundering and Terrorism Financing, Circular No 29 of 2006, (Jordan)

Regulations of Anti-Money Laundering and Terrorism Financing, Circular No 29 of 2006 (Jordan), [www.http://www.cbj.gov.jo/uploads/AML.pdf](http://www.cbj.gov.jo/uploads/AML.pdf).

Regulation of Investigatory Powers Act 2000 (UK) (RIPA)

Right to Financial Privacy Act of 1978, 12 USC § 3401

State Security Court Law No 17 of 1959, (Jordan) [Arabic] Official Gazette No 1429, on 1 July 1959, at 529

Telephone Consumer Protection Act of 1991, 47 USC § 227

Telecommunications Law No 13 of 1995 as amended by the Temporary Law No 8 of 2002, (Jordan) Official Gazette No 4416, 17 February 2000. The original law was issued in the Official Gazette No 4072, 1 October 1995

UK Data Protection Act of 1998

TREATIES

Agreement between the EFTA States and the Hashemite Kingdom of Jordan signed 21 June 2001 (entered into force 1 September 2002. EFTA States include: Iceland, Liechtenstein, Norway, and Switzerland. For text, see <<http://www.mit.gov.jo/Portals/0/efta/EFTA.pdf>> at 12 February 2011

Agreement between the Government of the Hashemite Kingdom of Jordan and the Government of Singapore on the establishment of a free trade area signed 16 May 2004 (entered into force 22 August 2005) For text, see <http://www.mit.gov.jo/Portals/0/Jordan_20Singapore_20FTA.pdf> at 12 February 2011

Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area (Jordan-US Free Trade Agreement (JUSFTA)) 24 October 1999 (entered into force 17 December 2001) http://www.mit.gov.jo/Portals/0/TextOA/AGREEMENT_TEXT.pdf

American Convention on Human Rights, opened for signature 22 November 1969 OASTS No 36 (entered into force 18 July 1978). For text see Organization of American States, Department of International Law, <<http://www.oas.org/juridico/english/sigs/b-32.html>>

Association Agreement Establishing a Free Trade Area between the Hashemite Kingdom of Jordan and the Republic of Turkey signed 1 December 2009 (entered into force 1 March 2011. For text, see <<http://www.mit.gov.jo/portals/0/JO%20EN%20Agreement%20Text.pdf>> at 12 February 2011

Cairo Declaration on Human Rights (CDHR) adopted Nineteenth Islamic Conference of Foreign Ministers, Cairo, 5 August 1990, UN GAOR, World Conference on Human Rights, 4th sess, agenda item 5, UN Doc A/CONF.157/PC/62/Add.18 (1993) [English trans] avail <<http://www.arabhumanrights.org/publications/regional/islamic/cairo-declaration-islam-93e.pdf>> at 4 February 2010

Convention for the Protection of Human Rights and Fundamental Freedoms ('European Convention on Human Rights' ('ECHR')), opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953)

http://www.hrcr.org/docs/Eur_Convention/euroconv3.html> at 10
January 2008

Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981) CE
<<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>> at 9
April 2010

EURO-Mediterranean Agreement: establishing an Association between the European Communities and their Member States, of the one part, and the Hashemite Kingdom of Jordan, of the other part, Official Journal of the European Communities, L129/3, Vol 45, 15 May 2002, avail <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:129:0003:0165:EN:PDF>

Free Trade Agreement between the Hashemite Kingdom of Jordan and Canada signed 28 June 2009. Text avail <http://www.mit.gov.jo> at 12 February 2011

International Covenant on Civil and Political Rights. Opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976)

Jordan-EU Economic Cooperation Association Agreement 1977 (entered into force 1978)

Jordan-EU Euro-Mediterranean Agreement, signed 24 November 1997 (entered into force 1 May 2002), OLJ L 129/3.

Ministry of Foreign Affairs, *Jordan and the Free Trade Agreement with the United States of America* <www.mfa.gov.jo>

Text on Non-Discrimination Adopted by the Article 31 Committee on May 31, 2000 <<http://www.ita.doc.gov/td/ecom/nondiscrimArt31May00.htm>> at 16 June 2010

Universal Declaration of Human Rights, GA Res 217A (iii), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948)

US-Jordan Joint Statement on Electronic Commerce
<http://www.jordanusfta.com/documents/joint_statement_on_e-commerce.pdf> at 10 November 2010

OTHER

Abu-Khasabeh, Suliman 'ATMs in Jordan', *Manabar Alrai* (Amman), 24 December 2010, Newspaper Article [Arabic], avail: <http://www.manbaralrai.com/?q=node/92420> at 19 January 2011

Aljazeera, US candid views on world leaders: US state department documents released by whistle-blowing website WikiLeaks provide

candid views on foreign leaders (2010) Aljazeera
avail<<http://english.aljazeera.net/indepth/spotlight/usembassyfiles/2010/11/2010112820116740589.html>> at 15 December 2010

Al-Rai, 'Surveillance Cameras Project', *Al-Rai* (Amman), 13 March 2009, [Arabic] <www.alrai.com> at 13 March 2009

APEC, 'APEC Privacy Framework' Fact Sheet (2010) <http://www.apec.org/en/About-Us/About-APEC/Fact-Sheets/Collection/APEC-Privacy-Framework.aspx> 27 November 2010

Arab Bank, 'Apply Now' online Application form (2009) <<http://www.arabbank.com.jo/en/applynow.aspx>> at 21 October 2009

Arab Bank, 'Internet Shopping' online Application form (2009) <<http://www.arabbank.com.jo/en/perscardinternet.aspx>> at 07 October 2009

Arab Bank, 'Privacy Policy' (2009) <<http://www.arabbank.com.jo/en/privacypolicy.aspx>> at 21 October 2009

Asia Pacific Forum, 'Jordan: Jordan National Center for Human Rights', (2010) <<http://www.asiapacificforum.net/members/apf-member-categories/full-members/jordan>> at 27 November 2010

Cairo Amman Bank, 'SMS Banking' (2009) <www.cab.com.jo> at 7 October 2009

Capital Investments, 'Banking Sector Report' (4 January 2009) <<http://www.capitalinv.jo/files/Banking%20sector%20Report-%204%20January%202009.pdf>> at 1 October 2009

Central Bank of Jordan, *Annual Report 2008* (2008) <<http://www.cbj.gov.jo/uploads/chapter2.pdf>> at 30 September 2009

Clarke, Roger, 'What's 'Privacy?' Paper prepared for an Australian Law Reform Commission Workshop (28 July 2006) <<http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html>> at 2 June 2009

Clarke, Roger, *Dataveillance by Governments: The Technique of Computer Matching* (1993) Xamax Consultancy Pty Ltd <<http://www.rogerclarke.com/DV/MatchIntro.html>> at 27 January 2010

Council of Europe, 'Council of Europe in Brief: Mission Objectives' <<http://www.coe.int/aboutcoe/index.asp?page=nosObjectifs&l=en>> at 9 April 2010

Department of Commerce (US), *EU Safe Harbour Overview*, US Department of Commerce < http://www.export.gov/safeharbor/eg_main_018236.asp > at 12 December 2010

Department of Commerce (US), *US-Jordan Free Trade Agreement (FTA)* (2009) US Commercial Service <<http://www.buyusa.gov/jordan/en/fta.html>> at 28 August 2009

Department of Commerce (US), *U.S.-EU Safe Harbor Framework* (2000) U.S. Department of Commerce <www.export.gov/safeharbor> at 5 July 2008

Department of Statistics, *Jordan in Figures: Selected indicators* (2008) Department of Statistics-Government of Jordan <http://www.dos.gov.jo/dos_home_e/main/jorfig/2008/jor_f_e.htm> at 23 December 2010.

'E-Government Study Finds Ease, Engagement, Privacy, Protection are Top Priorities', *PA Times* 26(5) (American Society for Public Administration, Washington, DC) May 2003, 2

Electronic Privacy Information Center [epic.org], 'The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report' <<http://epic.org/privacy/fcra/>> at 13 February 2010

ESIS, *Regulatory Developments in Jordan -Master Report: Jordan efforts to play a key role in the regional IT market* (2000) ESIS <<http://www.eu-esis.org/esis2reg/JOreg4.htm>> at 6 January 2011.

Estivill-Castro, Vladimir, Ljiljana Brankovic and David L Dowe, 'Privacy in Data Mining' (1999) 6(3) *Privacy Law and Policy Reporter* 22 <<http://www.austlii.edu.au/au/journals/PLPR/1999/44.html>> at 27 January 2010

European Commission, *EU/Jordan Action Plan* <http://ec.europa.eu/world/enp/pdf/action_plans/jordan_enp_ap_final_en.pdf> at 3 September 2009

European Commission, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (1998), working document DG XV D/5025/98 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf> at 16 June 2010

Federal Communications Commission, *Nationwide Do-Not-Call Registry* (2003) Federal Communications Commission <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-235841A1.doc> at 3 February 2010

Federal Financial Institution Examination Council, *Bank Secrecy Act/ Anti-Money Laundering: Examination Manual* (2006)

<http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf> at 25 February 2010

Federal Trade Commission , *In the Matter of Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens, File No. 052 3117, Docket No C-4161* (2006) Federal Trade Commission <http://www.ftc.gov/os/caselist/0523117/0523117NationsTitle_Complaint.pdf> at 03 March 2010

Federal Trade Commission, 'About the Federal Trade Commission' (2009) <<http://www.ftc.gov/ftc/about.shtm>> at 26 February 2010.

Federal Trade Commission, 'Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case' (News Release, 13 August 1998) <<http://www.ftc.gov/opa/1998/08/geocitie.shtm>> at 5 February 2010

Federal Trade Commission, 'Privacy Initiatives: Introduction' <<http://www.ftc.gov/privacy/index.html>> at 26 February 2010

Federal Trade Commission, 'Privacy Online: A Report to Congress' (1998) <<http://www.ftc.gov/reports/privacy3/index.shtm> > at 4 March 2010

Federal Trade Commission, 'Self-Regulation and Privacy Online' Testimony: Before the Subcommittee on Communications of the Committee on Commerce, Science and Transportation, US Senate, 27 July 1999, prepared statement by the Federal Trade Commission Chairman, Robert Pitofsky <<http://www.ftc.gov/os/1999/07/privacyonlinetestimony.pdf>> at 4 March 2010

Federal Trade Commission, 'The Gramm-Leach-Bliley Act: The Financial Privacy Rule' <http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html> at 3 March 2010

Federal Trade Commission, *United States of America (for the Federal Trade Commission) v. Rental Research Services, Inc., a corporation, and Lee Mikkelson, individually and as an officer of the corporation. FTC File No. 072 3228* (2009) Federal Trade Commission <<http://www.ftc.gov/os/caselist/0723228/090305rrscmpt.pdf>> at 03 March 2010

Finlan, Natasha Finlen, *Consumer Protection in the Australian Telecommunications Market-Post July 1997* (Legal Research Project Thesis, Macquarie University, 1997)

Foreign Ministry of Jordan, *Jordan and the European Union* (2008) <www.mfa.gov.jo> at 13 November 2008

Ghazal, Mohammad, 'King Launches e-Health Plan', *The Jordan Times* (Amman), 1 November 2009, avail <http://www.jordantimes.com/index.php?news=21113&searchFor=Hakeem> # at 24 December 2010

Gerasa News, *Convicted Offenders on Sexual Assault Charges: Taking Images of Minor's Underwear by a Mobile Phone [Arabic]* (2011) Gerasa News <<http://www.gerasanews.com/web/print.php?a=39651>> at 4 January 2011

Government of Jordan, *E-Government Program* (2003) Ministry of Information and Communications Technology <www.moict.gov.jo> at 15 November 2008

Government of Jordan, *E-Government Program* (2006) <www.jordan.gov.jo> at 30 April 2009

Government of Jordan, *Privacy Policy* (2009) The Government of Jordan <www.jordan.gov.jo> [Arabic] or <<http://www.jordan.gov.jo/wps/portal/MyEnglishPortal>> at 04 June 2009

Hamelink, Cees J, 'New Information and Communications Technologies, Social Development and Cultural Changes' Discussion Paper No 86 (United Nations Institute for Social Development, 1997)

HSBC, 'Privacy and Security: Your Privacy Matters to Us' (2009) <http://www.hsbc.jo/1/2/ALL_SITE_PAGES/privacy-and-security_hidden> at 23 October 2009

Hurley, Deborah, 'A Whole World in One Glance: Privacy as a Key Enabler of Individual Participation in Democratic Governance' (Paper presented at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13-14 September 1999<<http://www.pcpd.org.hk/english/infocentre/files/hurley-paper.doc>> at 29 July 2009

Jordan Ahli Bank, 'The E-Com Card' (2009) <http://www.ahli.com/prepaid_cards.shtm> at 07 October 2009

Jordan Economic & Commerce Bureau, 'Jordan & the WTO' (2005) Economic & Commerce Bureau, Embassy of Jordan, Washington, DC<http://www.jordanecb.org/agreements_jowto.shtm> at 10 July 2009

Jordan Investment Board, *Vital Sectors: ICT Sector* (2009) Jordan Investment Board <http://www.theodora.com/wfbcurrent/jordan/jordan_communications.html> at 10 July 2009

Jordan Kuwait Bank, 'Products and Services: Individual: Credit Cards' (2006) <http://www.jordan-kuwait-bank.com/en/products_individual_cards.html> at 9 October 2009

Jordan Kuwait Bank, 'Visa Electron to Replace Traditional ATM Cards' (2000) <<http://www.jordan-kuwait-bank.com>> at 7 October 2009

Kirby, Michael, 'Privacy Protection, A New Beginning: OECD Principles 20 Years on' (1999) 6 *Privacy Law and Policy Reporter* 25 <<http://www.austlii.edu.au/au/journals/PLPR/>> at 20 June 2009

Laudon, Kenneth C, 'Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information' Working Paper No 2451/1466, New York University, January 1997

Marto, Michel and Ziad Fariz, *Letter of Intent [of the Government of Jordan] and Memorandum on Economic and Financial Policies for 2000* (2000) International Monetary Fund <<http://www.imf.org/external/np/loi/2000/jor/01/index.htm>> at 9 July 2009

Middle East Newslite, *Jordan Develops EW Suite* (2008) Middle East Newslite <www.menewslite.com> at 08 December 2010

Ministry of Information and Communications Technology, 'About the MoICT' (2003) MoICT <http://www.moict.gov.jo/MoICT_about_moict.aspx> at 25 June 2009

Ministry of Information and Communications Technology, 'The E-Readiness Assessment of the Hashemite Kingdom of Jordan 2006' (2006) MoICT <http://www.moict.gov.jo/MoICT_Jordan_ereadiness.aspx> at 26 June 2009

Ministry of Information and Communications Technology, *E-Initiative Database* (2003) MoICT) <http://www.moict.gov.jo/MoICT/MoICT_Initiative.aspx> at 28 April 2009

Ministry of Information and Communications Technology, *Invest in ICT in Jordan* (2005) <<http://www.jordanecb.org/pdf/InvestinICTinJordan.pdf>> at 16 April 2009

Ministry of Planning and International Cooperation, *US Grant for Feasibility Study on Electronic Health Records in Jordan* (2010) Ministry of Planning and International Cooperation <<http://www.mop.gov.jo/arabic/>> at 24 December 2010.

O'Carroll, Lisa 'Phone-hacking Inquiry Extended to Include Broadcasters and Social Media' *The Guardian*, 20 July 2011,

<http://www.guardian.co.uk/media/2011/jul/20/phone-hacking-inquiry-broadcasters-social-media>

Office of Management and Budget, Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, Federal Register 54: 25818-25829 (1989) OMB <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf> at 3 February 2011

Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (2003) Office of Management and Budget <http://www.whitehouse.gov/omb/memoranda_m03-22/> at 30 December 2010

Organisation for Economic Co-Operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) OECD <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html> at 10 April 2010

Privacy International, *The Hashemite Kingdom of Jordan* (2007) <[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559523](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559523)> at 30 June 2010

Rotenberg, Marc (1998) 'Self-Regulation Won't Work', *USA Today* (McLean, VA), 7 July 1998, www.usatoday.com

Royal Jordanian, *Privacy Policy* (2009) Royal Jordanian Airlines (23 June 2008) <<http://www.rj.com/en/tabid/214/Default.aspx>> at 4 June 2009

Singleton, Solveig Singleton, 'Privacy and Human Rights: Comparing the United States to Europe' (White Paper prepared for the 'Rights, Rules and Regulations: The Future of Financial Privacy' Conference of the Competitive Enterprise Institute, Washington DC, 30 November – 1 December 1999) CATO Institute <<http://www.cato.org/pubs/wtpapers/991201paper.html>> at 08 April 2010

Spot On Public Relations, *Middle East and North Africa Facebook Demographics* (2010) Carrington Malin <http://www.spotonpr.com/wp-content/uploads/2010/05/FacebookMENA_24May10.pdf> at 22 December 2010

Standard Chartered Bank Jordan, 'Data Protection & Privacy Policy Statement' (2006) <<http://www.standardchartered.com/jo/data-protection-privacy-policy/en/>> at 23 October 2009

Stewart, Blair, 'Privacy Impact Assessment' [1996] *Privacy Law and Policy Reporter* 39
<<http://www.austlii.edu.au/au/journals/PLPR/1996/39.html>> at 1 July 2009

Telecommunications Regulatory Commission (Jordan), 'Consumer Guidelines' (2009) <www.trc.gov.jo> at 10 December 2009

Telecommunications Regulatory Commission (Jordan), *Privacy Policy* (2009) Telecommunications Regulatory Commission
http://www.trc.gov.jo/index.php?option=com_content&task=view&id=523&Itemid=1026&lang=english > at 04 June 2009

The Executive Privatization Commission, 'Mandate and Tasks' (2009) <<http://www.epc.gov.jo/EPC/Home/Mandatetasks/tabid/81/Default.aspx>> at 9 July 2009

United States Agency for International Development, *USAID/Jordan Strategy 2004-2009: Gateway to the Future (US Agency for International Development, 2003)* <http://pdf.dec.org/pdf_docs/PDABZ632.pdf> at 20 November 2008.

US Department of Commerce, 'Safe Harbor Overview' (1 January 2010) <http://www.export.gov/safeharbor/eg_main_018236.asp> at 17 June 2010

US Department of Commerce, 'U.S.-EU Safe Harbor Frameworks' (2000) U.S. Department of Commerce <www.export.gov/safeharbor> at 05 July 2008

US Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973) HEW <<http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>> at 16 February 2011

US Government, *Privacy and Security* (2010) US Government <http://www.usa.gov/About/Privacy_Security.shtml> at 24 December 2010.

World Trade Organisation, 'Jordan becomes 136th member of the WTO' (Press Release No 174, 11 April 2000) <www.wto.org/english/news_e/pr174_e.htm> at 25 June 2009

World Trade Organisation, *Reference Paper: Negotiating group on basic telecommunications* (24 April 1996) WTO <http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm> at 23 January 2011

World Trade Organisation, *WTO News: WTO successfully concludes negotiations on China's entry* (2001) WTO
<http://www.wto.org/english/news_e/pres01_e/pr243_e.htm> at 23
January 2011

Wright, Stephen and Rebecca English, 'Editor Charged in the Royal Phone-Hack Affair' *Mail Online*, 9 October
2011<<http://www.dailymail.co.uk/news/article-399896/Editor-charged-royal-phone-hack-affair.html>>


APPENDICES

Appendix A

Exhibits 1-3

Exhibit 1

www.jordan.gov.jo



Jordan
The Official Site of the Jordanian e-Government

عربي | [FAQ](#) | [ASK](#) | [Site Map](#) | [Help](#)

[Home](#) > [Privacy Policy](#)

Privacy Policy

1. This is a Government of Jordan Portal (hereinafter: the Website). Thank you for examining our privacy statement.
2. If you are only browsing this Website, we do not capture data that allows us to identify you individually such as your name, phone number or e-mail address. We would only obtain this type of information if you supply it by sending us an e-mail or registering in a secure portion of the Website. We also obtain this information when you send any queries to us.
3. If you choose to make an application or send us a query e-mail for which you provide us with personally identifiable data, we may share necessary data with other Government agencies, so as to serve you in a most efficient and effective way, unless such sharing is prohibited by legislation. We will NOT share your personal data with non-Government entities, except where such entities have been authorized to carry out specific Government services.
4. In case any information is collected, it shall be used improve the content of our Website and to personalize the content for you. It may also be used to notify our users about any updates for our website.
5. This website does not normally use "cookies" to track how our visitors use this site or to determine sites previously visited. If cookies are in use and you have your cookies notification option activated on your browser the system will notify you before any cookies are used so that you may refuse them. This will slow down your online experience and prevent you from utilizing certain features of this Portal. (A "cookie" is a file that may be placed on your hard drive without your knowledge by a Web site to allow it to monitor your use of the site.). Under no circumstances will the Government use any type of cookie to:
 - a. Retrieve any information from your computer that is not part of the cookie we sent to you;
 - b. Write any code, as part of the cookie, that could be harmful to your computer.
6. To safeguard your personal data, all electronic storage and transmission of personal data are secured with appropriate security technologies. This Website employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. This software receives and records the Internet Protocol (IP) address of the computer that has contacted our Website, the date and time of the visit and the pages visited. We make no attempt to link these addresses with the identity of individuals visiting our site unless an attempt to damage the site has been detected.
7. This Website may contain links to other Government and non-Government websites whose data protection and privacy practices may differ from ours. We are not responsible for the content and privacy practices of these other websites and encourage you to consult the privacy notices of those sites.
8. The Government will continually review and up-date its security procedures as new technologies become available and new activities are introduced. Any third party to whom the information is transferred should be made aware of these security practices and is also required to take reasonable precautions to protect the transferred information.
9. The Government takes all reasonable measures to ensure that the information it holds is accurate. In particular it uses reliable collection methods and destroys or converts to an anonymous form any out-of-date data.

[About Us](#) [Privacy Policy](#) [Terms Of Use](#)
Copyright © 2006 - 2010 Government of Jordan. All rights reserved.

Exhibit 2

<http://www.trc.gov.jo>



- › Home
- › About TRC
- › Laws & By-Laws
- › Regulations
- › Consultations
- › Regulatory Framework & Services
- › Radio Frequency Spectrum
- › Licensing
- › Equipment
- › ICT & Postal Markets
- › Tenders
- › Consumer Information
- › Media & Communications
- › Publications
- › TRC Employees
- › Contact Us



- General privacy policy
- Security terms
- Disclaimer of liability
- Management responsibilities
- Protection of personal information
- Registration forms
- Copyright
- Free services
- Other sites
- How can you help protect your information?
- How does the TRC handle concerns or complaints?
- What else you need to know about privacy at TRC?
- Contacting the web site
- Governing law

General privacy policy

TRC is sensitive to privacy issues on the internet and is committed to protecting your online privacy on The **Top** website. TRC believes that privacy is important to the success and use of the internet. This statement demonstrates our firm commitment to privacy and describes the practices that TRC will follow with respect to the privacy of users of this site. TRC reserves the right to change this privacy statement at any time by notifying visitors to this web site of the existence of a new privacy statement. Accordingly, please check back periodically. Privacy statement is accessible from the footer of each page. The following discloses the information gathering and dissemination practices for this web site: <http://www.trc.gov.jo>

Security terms

In order to ensure that this web site remains available to all users, the TRC may monitor network traffic to identify unauthorized attempts to upload or change information or to otherwise cause damage to the site. Anyone using this site expressly consents to such monitoring. And unauthorized attempts to modify, alter, deface, destroy or corrupt any information stored on this site or this system, to defeat or circumvent any security features, to probe, scan or test for vulnerabilities, to breach security or authentication measures, to forge tcp/ip headers, to install or attempt to install unauthorized software, to mount denial of service attacks or to utilize this system for other than its intended purposes are expressly prohibited and may result in criminal prosecution. At the other hand, any possible criminal activity will be reported, together with any evidence which may be gathered, to the appropriate authorities.

Disclaimer of liability

Every effort is made to provide useful, accurate and complete information. However, we cannot guarantee that there are no errors. The TRC makes no claims, promises or guarantees about the accuracy, completeness, usefulness or adequacy of the contents of this site and expressly disclaims liability of any sort for errors and omissions in the contents of this site. By the way, neither the TRC, nor its employees, associates nor contractors make any warranty, expressed, implied or statutory, including, but not limited to, any warranty that third party rights or title have not been infringed, or any warranty of merchantability or fitness for any particular purpose. And also no warranty of any sort is made with respect to the content of third party sites that have links from this site and all liability of every sort is expressly disclaimed. Actually, TRC is not liable in any circumstances for special, indirect or consequential damages or any damages whatsoever resulting from loss of use, loss of data or loss of revenues or profits, whether in an action of contract, negligence or otherwise, arising out of or in connection with any use of the information or services available on this site.

Management responsibilities

Management must make reasonable efforts to ensure that all private information is used only as intended, and that precautions preventing misuse are both effective and appropriate. Management is responsible for establishing appropriate controls to ensure that private information is disclosed only to those who have a legitimate business need for such access. Management must establish and maintain sufficient controls to ensure that all TRC information is free from a significant risk of undetected alteration.

Protection of personal information

Personal information means any information that may be used to identify an individual, including, but not limited to, a first and last name, email address, a home, postal or other physical address, other contact information, title, industry, and other such information.

In general, you can visit and browse the TRC website to access information while remaining anonymous and not revealing any personal information. There are times, however, that we will ask you to provide certain information (such as your name and address) so that we may provide technical support assistance, to fulfill your request for TRC to make you aware of any new news or services that you might be interested in.

TRC collects personal information when you register with TRC for TRC account (member area), when you use TRC services or make an inquiry, when you ask to be included in mailing list, or when you submit your information to TRC for any other reason. When personal information is collected, we will inform you at the point of collection the purpose for the collection. TRC does not intend to transfer your personal information to third parties without your consent. Such consent will be considered granted to TRC upon acceptance of the eula ("end user license agreement").

Forms you fill out to interact with our business units may request that you give us sensitive information such as your e-mail address, mailing address, telephone number. Whenever that is the case, TRC will take all commercially reasonable steps to establish a secure connection with your web browser.

Registration forms

Telecommunications regulatory commission currently has many type of registration for job applicant, member's area, and others databases.

How your personal information is used by TRC?

Personal information is only used by TRC for the purposes stated at the time of collection or as otherwise set out in this section.

Non-personal aggregate information may also be extracted or compiled from the information we collect. Such information may be used to generate statistics and aggregate reports for internal use by TRC. In this instance, these statistics and reports will contain only aggregated and no personally identifiable information. Your identity is kept strictly anonymous.

Copyright

All content on this site, and all content of any documents provided to visitors or clients (in, for instance, newsletters, news) is the property of the TRC, unless stated otherwise. And no user may modify, publish, transmit, transfer or sell, reproduce, create derivative works from, distribute, display, or in any way exploit any of the content, in whole or in part, except with the express written agreement of the TRC.

Free services

The TRC provides a number of free services from its site, such as newsletters, polls, press room etc. There is no contract with the TRC for any free service, so no user can become a client by using any free service and the TRC is not liable to any user in any way resulting from use of any free service.

Changes in this privacy statement

If we change this privacy statement in ways that affect the personally identifying information we have collected through our sites, we will post those changes in this space and advise you of choices you may have as a result of those changes. We will also post a notice on our home page that this privacy statement has changed.



Other sites

TRC websites may contain links to other sites, including those of business related. While we seek to link only to sites that share our high standards and respect for privacy, we are not responsible for the privacy practices employed by other sites.

How can you help protect your information?

If you are using a TRC web site for which you registered and chose a password, we recommend that you do not divulge your password to anyone. We will never ask you for your password in an unsolicited phone call or in an unsolicited e-mail. Also remember to sign out of the registered site and close your browser window when you have finished your work. This is to ensure that others cannot access your personal information and correspondence if others have access to your computer.

How does the TRC handle concerns or complaints?

The TRC believes that individuals should have the right to review their personal information to ensure its accuracy. To review the information submitted to the TRC, users can contact the TRC at TRC@TRC.gov.jo or  [+\(962\) 65501120](tel:+96265501120) .

What else you need to know about privacy at TRC?

TRC websites are committed to maintaining and protecting your privacy as a visitor to this website. However, we remind you that the internet is not a secure medium. As such, your privacy cannot be guaranteed when you communicate online or otherwise visit any website. The nature of internet communications means that your communications may be susceptible to data corruption, interception and delays.

Contacting the web site

If you have any questions about this privacy statement, the practices of this site, or your dealings with this web site, you can contact us via our feedback form.

Governing law

These terms shall be governed by and construed in accordance with the laws of the Hashemite kingdom of Jordan and the user explicitly accepts that only the law courts of Jordan have jurisdiction to deal with any matter arising from or in any way, whether directly or indirectly, related the use of this website and, accordingly, the user explicitly waives all and any rights to bring any action of any sort in relation to this web site in any court anywhere else in the world.

Top

| [E-Gov](#) | [Site Map](#) | [Members Area](#) | [subscribe to our mailing list](#) |

[Privacy Policy](#) [Terms of usage](#)

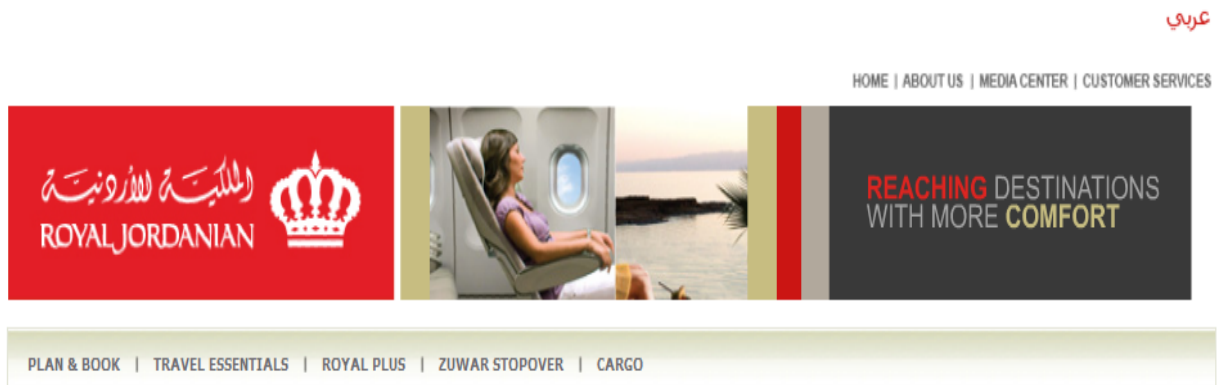
Copyright ©2010, Telecommunications Regulatory Commission. All Rights Reserved.

Developed By : [Batelco Jordan](#)

[Top](#)

Exhibit 3

www.rj.com



Privacy Policy

Your privacy is important to Royal Jordanian Airlines and we want you to know that the information we collect will be treated with care. This privacy Policy applies to all information collected by Royal Jordanian when you are on this site and when you utilize any service provided by Royal Jordanian. We will only use your information in accordance with this Policy. Your use of this website constitutes your agreement to this Privacy Policy. By using this website, you are agreeing on the terms of this Privacy Policy and that your personal information may be sent and processed by Royal Jordanian or suppliers and third parties exclusively providing services for Royal Jordanian Airlines in countries with varying applicable data protection laws.

Collection of personal information

When you visit the Royal Jordanian Airlines website, we may collect and store information about your visit on an anonymous, aggregate basis. This information may include the time and length of your visit, the pages you look at on our sites, and the site you visited just before coming to ours. We may also record the name of your Internet service provider. We use this information only to measure site activity and to develop ideas for improving our sites.

There are also several opportunities on our websites for you to provide us with information about you and your preferences. The types of personal information you provide to us on the pages of this website may include, but is not limited to, contact information such as your name, address, telephone number, and email address; financial information such as your credit card number; and other unique information such as user IDs and passwords, billing and transaction information, product and service preferences and tracking statistical information. If you choose to share any personal information with us, we may store it and use it for marketing research and other marketing purposes.

How we use your information

Royal Jordanian collects your information to understand your needs and interests, complete transactions and fulfill requests for our services. We may use your information for:

- ▶ Assisting you in making reservation to purchase airline ticket or related product and Services available on our website;
- ▶ Communicating with you about personalized promotional offers;
- ▶ Updating you on new services and benefits;
- ▶ Contacting you for market research regarding our offers or services.

- ▶ Administrative and analytical purposes such as information system management, accounting, billing and audits, marketing, credit card processing and verification, customer relations correspondences, and/or our frequent flyer (Royal Plus) Program.

The information you share with us may be used by Royal Jordanian Airlines and its partners. We may share your personal information with our suppliers and third parties exclusively to provide services for Royal Jordanian Airlines or to fulfill the services you have requested, and with our business partners exclusively to conduct joint marketing programs with Royal Jordanian Airlines. **We will not share your personal information with other third parties for their independent use without your permission.** We will not use or share your information except in compliance with this Policy.

To the extent required by law, we may disclose personal information to government authorities, or to third parties pursuant to a legal process.

Information We May Place Automatically On Your Computer's Hard Drive

Our website may make use of "cookie" technology to measure site activity and to customize information to your personal tastes. A cookie is an element of data that a Website can send to your browser, which may then store the cookie on your hard drive. So, when you come back to visit us again, we can tailor information to suit your individual preferences. The goal is to save you time and provide you with a more meaningful visit.

Newsletters

You only receive our newsletter after you subscribe to this service on the website. Newsletters may include information from our business partners. If you subscribed to our newsletter but do not want to receive it in the future, please follow the "unsubscribe" instructions contained in the newsletter, which includes an individualized link to your subscription information.

Links to other website

Our website may contain links to other websites not maintained by Royal Jordanian. Other websites may also reference or link to our website. These links will lead you to sites that are not maintained by us and may operate under different privacy practices. You are responsible for reviewing the privacy statements for such other websites, as we have no control over information that is submitted whilst visiting such sites.

Minors

Royal Jordanian does not knowingly collect personal identifiable information from minors. If you are a Parent or Guardian of someone who is, according to the applicable law, minor and has provided us with information without your knowledge and consent, you may request that we remove this information by contacting us at or email address RJ@RJ.COM

Who to Contact

If you have previously submitted Personal Data through the Site and would like that information deleted from our records and database, please contact us at our email address: RJ@RJ.COM

We will use every reasonable effort to delete this information from our existing files and confirm with you the deletion of your Personal Data.

Privacy Modifications

Royal Jordanian reserves the right to change this Privacy Policy at any time. We will post any changes here, so be sure to check back periodically. Use of the website after the effective date of modifications constitute acceptance of the modified terms and conditions of this policy. This policy was last updated on June 23, 2008.

Copyright (c) 2009 Royal Jordanian Airlines | Privacy Policy

Latest News : Khartoum daily, starting from 17 September



Jordan Links | Contact Us | Legal Disclaimer | Privacy Policy | FAQ | Currency Converter | Sitemap | Careers | Search

Appendix B

Exhibits 1-9

Exhibit 1

www.jo.zain.com

Home | About us | Sitemap | Careers | Contact us | عربي

zain Jordan Login | Register

Search

Media Center Personal Business Entertainment Youth Internet Support My Account

Zain Privacy Policy

[Print this page](#)
[Send this page](#)

Zain Privacy Policy

Our Privacy Undertaking:
WE RESPECT YOUR PRIVACY REGARDLESS OF THE MEDIA IN WHICH WE COMMUNICATE, YOUR INFORMATION IS SAFE WITH US

Scope

This privacy policy "Privacy Policy" describes what type of the personal information we collect from you and how we may use this information. Please read it in conjunction with the legal terms and conditions on Zain web and WAP sites and any other terms related to other products or services.

Your Personal Information

Personal information is any data that identifies you in person. This information should be true, complete updated and accurate at all times and you hereby agree to update your information and your profile regularly.

If, at any time, you wish to update or amend the personal information you have submitted on the site, you can do so online by visiting the "My Profile" section or by contacting our call centre where we will assist you in doing so.

Personally identifiable information collected by us shall be dealt with in strict confidentiality. We collect personally identifiable information from you when you become a Zain customer, when you visit or register at the Zain Portals (WEB, WAP and/or when you enrol in any other service or product that we introduce), when you purchase from any of our shops or through our dealers and sub-dealers, when you enter any promotions or competitions on our portals or through our Rassel channels, IVR..., when we call you, or otherwise. We collect your personal information because we want to serve you customised offers and to enhance your user experience with us.

The type of personal information we may collect could include, for example, your name and postal address, date of birth, gender, telephone and fax numbers, email address and more.

In summary, we may use your personal information to:

Evaluate and develop online and offline new products and services and notify you of the roll-out of new features, products, services and special offers.
Process the transactions you enter into with us or others through our portal. We might disclose personal information to a third party to the transaction, but only to process your transaction.
Inform you of any products and services offered by other companies that we think may be of interest to you, provided that you choose to opt in to receive this information from them.
Collect payments from you.
Verify that you are an authorised user if you contact us, call our helpdesk or call centre.
Inform you of any service related changes affecting your use of our site or any of our services.
Provide personalised services that meet your needs on our portal. We may collect personal information about your usage of the services and your navigational habits.
Communicate with you to gather research information that will assist us in conducting market analysis. This is intended to enhance and improve our services to you and to better market our products and services.

We may disclose personal information if required to do so by law or in the good-faith intention that such action is necessary to (a) conform to the edicts of the law or comply with legal process served on us or our affiliates; (b) protect and defend our rights or property or those of our subscribers, and (c) act as immediately necessary in order to protect the personal safety of our subscribers or the public.

We may disclose your information to other companies who are the legal owners of Zain, including their respective partners, agents and sub contractors, for any of the above purposes.

Deals with Third Parties

We enter into agreements and business relations with other companies and trusted third parties ("Third Parties"). These companies can be content providers, solutions providers, business partners or otherwise. We team up with them to offer you different services and solutions.

Accordingly, we use your personal information to operate the sites and services that we offer, and to inform you of new features, services, and products available to you. The use of information will remain under our control and monitored by us at all times.

As well, you might opt-in to receive information from these companies and we may sometimes disclose your personal information to those companies provided that they are under the legal undertaking to use your personal information within the scope permitted herein. Should you decide that you no longer wish to receive information from a particular company, you should contact that company directly.

In case you decide to disclose your personal information to another company, our privacy policy will no longer apply and the third party's privacy policy shall be applicable.

We may disclose your personal information such as your name, account and mobile phone in the event that we undergo re-organization or are sold to a third party.

If you are a registered user, any messages you send to an email address, including whether from your phone or from the portal, might include any or all of: Your registered site First name, Last name, Username (email address), Chat nickname, your phone number and more.

You acknowledge that by providing your information and data to us, you consent to the processing of your data in accordance with this Privacy Policy.

Communicating With You

We will be communicating with you and contacting you in several manners, whether by email, SMS, MMS, direct calls or otherwise.

Cookies

Cookies are pieces of information placed by some websites on your computer. It identifies your computer whenever you visit that web site, in order to provide you with enhanced online experiences. Zain may create cookies when you visit our sites.

Cookies may be used to help you in the following ways:
to identify your personalised settings, and offer you customised information
to control serving banner advertising or announcements on the site;
to run statistics and generate records of how many times you do specific things on the site,
to track where you have come from if you were referred to our website;
and to make our email offers more relevant to you by taking into account your response to previous email offers.

Our cookies will not be used to analyse your visits to other sites.

Information Security

Communication and messaging over the Internet is not secure unless it is encrypted, for example chatting, emails/webmails, messaging and more. Your communications may route through a number of countries and cyber locations before reaching its destination and this is the nature of the Internet. Zain shall not be responsible for any unauthorised access or loss of personal information that is beyond our control.

Legal Disclaimer and Limitations of Liability

As mentioned in our Legal Terms and Conditions:

The Service is supplied to you on an "as is" and "as available" basis. We make no warranties, express or implied, with respect to the Service and/or the Content whatsoever (including without limitation regarding their quality, merchantability, fitness for a particular purpose, suitability, reliability, timeliness, accuracy, completeness, security or that they are free from errors) unless specifically set out in these Terms or any other applicable terms.

We use our reasonable endeavors to ensure that the information within the Service is accurate at the time of its inclusion, but your access to the Service and any action you carry out on the basis of data or information you obtain from or via the Service (including any transaction you make with a third party for the supply of goods or services to you) is carried out entirely at your own risk and we accept no liability for any losses that you may suffer as a result. The inclusion of links on the Service to third party sites not controlled by us does not imply any endorsement by us of such sites. The Service is provided to you through a variety of systems (including telecommunications) and we are unable to guarantee error-free use or transmission of, or access to, any part of the Service.

Accordingly, we shall not be liable for any costs, expenses, loss of use, profits or data or any indirect, special or consequential damages or losses, whether such losses or damages arise in contract, negligence or tort, including without limitation to the foregoing any losses in relation to:

your use of, reliance upon or inability to use our Service and/or Content;
the deletion with or without notice or cause of any of your data or information stored on the Service;
any loss of your data or material resulting from delays, non-deliveries, missed deliveries, service interruptions or a failure, suspension or withdrawal of all or part of the Service at any time; or
the removal from the Service of any material sent or posted by you on or via the Service and/or the blocking or suspension of your access to the Service or any part of it in accordance with these Terms.

If you are dissatisfied with any part of the Service or with any of these Terms, your sole and exclusive remedy is to discontinue using this Service.

Third Party Sites

This privacy policy does not apply to third party sites that you may access from our site. You should therefore read their privacy policy fully before you use their services.

Changes to Privacy Policy

Zain reserves the right to amend or modify this Privacy Policy at any time and in response to changes in applicable data protection and privacy legislation.

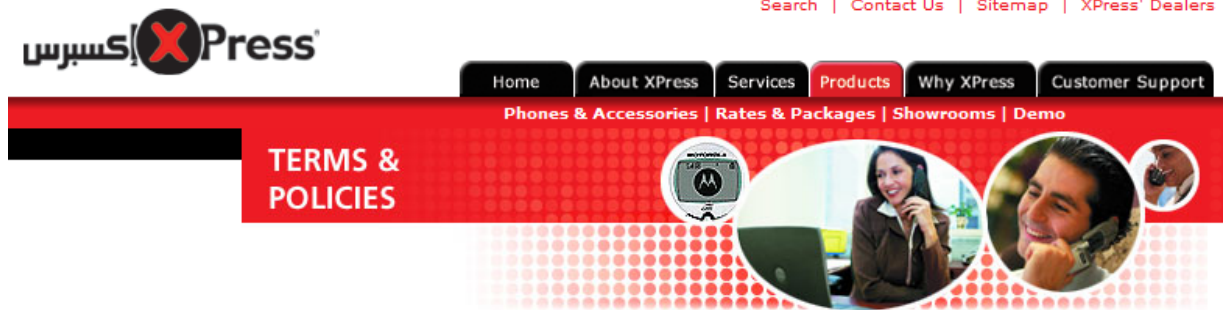
Contact Us Immediately

If you have any questions about the handling or protection of your personal information, please contact us.

DATE REVISED: 08/09/2007

Exhibit 2

<http://www.xpress.jo/terms/terms-policies.asp>



Terms of Use for www.xpress.jo

XPress requires that all persons or entities visiting any XPress sites on the World Wide Web agree to the following terms and conditions. By accessing this website, you confirm your agreement to and acceptance of the following terms and conditions:

Copyright Notice

Copyright ©2004 XPress Telecommunications. All rights reserved.

Your Use of Information

The materials available on this website, unless otherwise specified, are the property of XPress or its licensors, and are protected by copyright, trademark and other intellectual property laws. To the extent that XPress has the right to do so without compensation to third parties, and except for materials or information specifically provided under other terms, XPress grants you permission to copy or otherwise download from its website, information and materials (including related graphics), on the condition that:

1. The materials are for internal, private and non-commercial use only.
2. Any copies of materials or portions thereof must include the copyright notice specified on the website (see above).

If attribution to XPress is included, limited quotations from the content are hereby permitted. You may not copy or display for redistribution to third parties for commercial purposes any portion of the content without the prior written permission of XPress.

Documents and information posted by XPress on this website may contain other proprietary notices or describe products, services, processes or technologies owned by XPress or third parties. Nothing contained herein shall be construed by implication or otherwise as granting to the user a license under any copyright, trademark, patent or other intellectual property right of XPress or any third party.

Trademarks

The XPress name and logo and all related product and service names, design marks and slogans are trademarks, service marks or registered trademarks of XPress and may not be used in any manner without the prior written consent of XPress. Other products and service marks are trademarks of their respective owners.

Consent to Monitoring and Disclosure

XPress is under no obligation to monitor the information residing on or transmitted to this website. However, anyone accessing this site agrees that XPress may monitor the site to:

1. Comply with any necessary laws, regulations or governmental requests.
2. In its sole discretion, operate the website in a manner it deems proper or to protect against conduct it deems inappropriate.

XPress shall have the right, but not the obligation, to reject or eliminate any information residing on or transmitted to this website that it, in its sole discretion, believes is unacceptable.

Limitation of Liability

You assume all responsibility and risk for the use of this website and the Internet generally. In no event shall XPress or its affiliates be liable for any direct, special, indirect or consequential damages or any damages whatsoever; including but not limited to loss of use, data or profits, without regard to the form of any action; including but not limited to contract, negligence or other tortious actions, arising out of or in connection with the use, copying or display of the content resulting from access to or use of this website; or the Internet generally, under contract, tort or any other cause of action or legal theory.

Although XPress believes the content to be accurate, complete and current, XPress makes no warranty as to the accuracy, completeness or currency of the content. It is your responsibility to verify any information before relying on it. The content of this website may include technical inaccuracies or typographical errors. From time to time, changes are made to the content herein. XPress may make changes in the products and/or the services described herein at any time.

Warranty Disclaimer

If you access this website or rely on any material available through it, you do so at your own risk. You agree that you are solely responsible for any damage to your computer system or loss of data that results from any materials downloaded from or otherwise provided through this website. Access to this website (including any information or materials therein) is provided on an "as is" basis, without warranties of any kind, either express or implied, including, but not limited to, warranties of title or non infringement.

No advice or information given by XPress, its affiliates or their respective employees shall create any warranty. Neither XPress nor its affiliates warrant that the information or materials on, or access to, any site will be without interruption, error free or that it will be free of viruses or other harmful components.

Endorsements and Linked Sites

Some of the sites listed as links herein are not under the control of XPress. Accordingly, XPress makes no representations whatsoever concerning the content of those sites. The fact that XPress has provided a link to a site is NOT an endorsement, authorization, sponsorship or affiliation by XPress with respect to such site, its owners or its providers. XPress is providing these links only as a convenience to you. XPress has not tested any information, software or products found on these sites and therefore cannot make any representations whatsoever with respect thereto.

You agree that you will comply with any security processes and procedures (such as passwords) specified by XPress with respect to access to or use of this website. Further, you agree not to access or attempt to access any areas of or through this website which are not intended for general public access, unless you have been provided with explicit written authorization to do so by XPress.

Changes and Other Terms

XPress has the right to make changes and updates to any information contained within this website without prior notice. XPress reserves the right to change any of the Terms of Use without prior notice. Access to particular areas on this website may be subject to additional or different terms and conditions, as specified by XPress from time to time.

Failure to Comply

XPress has the right to terminate or restrict your access to some or all of this website, unilaterally and without notice, in the event that you violate any of these Terms of Use. XPress also reserves any and all remedies at law or equity in connection with violation of these Terms of Use.

Information Provided by You

Except as provided below, any unsolicited information provided by you, that does not contain individually identifiable information, including but not limited to unsolicited feedback, data, questions, comments, suggestions or the like shall be deemed to be non-confidential.

XPress shall have no obligation of any kind with respect to such unsolicited information and shall be free to reproduce, use, disclose and distribute the information to others without limitation, except for information that is personally identifiable.

Additionally, XPress shall be free to use any such unsolicited ideas, concepts, know-how or techniques contained in such information for any purpose whatsoever, including but not limited to developing, manufacturing and marketing products incorporating such information.

XPress' use of any individually identifiable information provided by you shall be governed in accordance with XPress' Privacy Policy.

Governing Law

These Terms of Use shall be governed by and construed in accordance with the laws of the Hashemite Kingdom of Jordan. The Courts of Center Amman shall have the exclusive jurisdiction in all disputes and actions relating to these Terms of Use.

Indemnification

You agree to indemnify, defend and hold harmless XPress and any third party information providers for this website from and against all liabilities, losses, expenses, damages and costs, including reasonable attorneys' fees, arising from: (1) any violation of these Terms of Use by you; (2) any violation of any rights of a third party; (3) any violation of applicable law or regulation; (4) information or Content that you submit, post, transmit or make available through this website, or (5) your use of this website.

Severability

If any provision of These Terms of Use shall be deemed unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from these terms and conditions and shall not affect the validity and enforceability of any remaining provisions.

Exhibit 3

<http://www.umniah.com/umniah>

Privacy Policy

Effective December 2009 until amended.

Welcome to the website of Umniah Mobile Company and Al Bahrania Al Urdunia Liltaknia Wa Alitaisalat ("Batelcc Jordan") (collectively and severally referred to as "Company"). Please read this privacy policy ("Policy") carefully. These are the privacy policy terms that describe what information about you is collected and how that information may be used, disclosed, and protected when you access this website ("Site") or use any of the Services. If you do not agree with them, you should not proceed any further on the Site. By continuing to browse, use the Site and/or any of the Services shown on the Site, you confirm that you agree to be bound by this Policy.

This Policy should be read in conjunction with the [Terms and Conditions](#) of use for the Site.

1 **Personal Information & Data**

You hereby consent and acknowledge that by providing information and data to The Company, you consent to the processing of your information and data in accordance with this Policy.

1.2 **Type of Collected Data**

- 1.2.1 The type of personal information and data The Company may collect shall include but not be limited to:
 - Your name and postal address
 - Date of birth
 - Gender
 - Telephone and fax numbers
 - Email address
 - Other information collected on registration or through surveys.
 - 1.2.2 The Company may request you to provide additional information such as your credit card number and billing address if you choose to access and/ or download any Services that require a charge.
 - 1.2.3 The Company may collect information about your visit and use of the Site and/ or Services, including the pages you view, the links you click and other actions taken in connection to the Site and/ or Services. The Company shall also collect certain standard information that your browser sends to every website you visit, including but not limited to your IP address, browser type and language, access times and referring web site addresses.
- #### 1.3 **Use of Collected Data**
- 1.3.1 The data collected by The Company will be used for purposes including but not limited to:
 - Operation and improvement of the Site and the delivery of the Services.
 - Carrying out of any transactions you may have requested and the collection of any payments due from you.
 - Performance of research and analysis aimed at improving The Company products, services and technologies.
 - Display of content and advertising that are customized to your interests and preferences.
 - Communicating with you including but not limited to certain mandatory service communications such as welcome letters, billing reminders, information on technical service issues, and security announcements.
 - 1.3.2 Information and data collected by The Company through the Site and Services may be stored and processed anywhere The Company sees fit. By using the Site and/ or Service, you consent to any such storage and/ or transfer of information and data by The Company.
- #### 1.4 **You hereby declare and warrant the following:**
- 1.4.1 All the information you have provided is true, accurate, current and complete.
 - 1.4.2 The information and/ or material you have provided is fit for publication and that you hereby undertake to indemnify The Company if any third party takes action against The Company in relation to the information and/ or material that you submit.
 - 1.4.3 You warrant that The Company may publish the information and/ or material you submit and/or make use of it or any concepts described in it in The Company products or Services without liability and you agree not to take action against The Company in relation to it.

- 1.4.4 You hereby consent and acknowledge that The Company may disclose your information and data to third parties for the performance of specific tasks. Such parties will be permitted to obtain only the information they need to perform their tasks, and they will be required to maintain the confidentiality of the information and are prohibited from using it for any other purpose.

2 Data Security

- 2.1 Although The Company makes every effort to ensure the security of your data and communications, you are however advised that for reasons beyond The Company's control, there is a risk that your communications may be unlawfully intercepted or accessed by those other than the intended recipient. You hereby acknowledge that The Company is unable to exercise control over the security of the Site passing over the Site or via the Services and The Company hereby excludes all liability of any kind for the transmission and/ or reception of infringing content of whatever nature or for any unauthorized access or loss of information and data that is beyond the reasonable control of The Company.
- 2.2 If a password is used to help protect your accounts and personal information, it is your responsibility to keep your password confidential. Do not share this information with anyone. If you are sharing a device with anyone you should always choose to log out before leaving a site or service to protect access to your information from subsequent users.
- 2.3 The Company may monitor and/ or record your emails, text messages or other communications that take place on the Site for security and/ or quality control purposes in accordance with the applicable laws for the purposes of preventing unauthorized use of The Company's Site and/ or systems.

3 Use of Cookies

- 3.1 Cookies are text files that are placed on your hard disk by a web page server, these text files contain information that can later be read by a web server in the domain that issued the cookie to you. Cookies cannot be used to run programs or deliver viruses to your device.
- 3.2 Cookies are used by The Company to store your preferences and to help you save time and provide you with a more personalized service on our Site without the constant need to re-enter the same information when you return to a specific web page.

- 3.3 You may choose to accept or decline cookies. Although most web browsers automatically accept cookies, you may be able to modify your browser setting to decline cookies if you prefer. Declining cookies may result in the inability to sign in and/ or inaccessibility to some of the Site's features.

- 3.4 If you are using a public or shared device and do not want this information to be stored, we advise you to delete any cookies that may have been stored on the device.

4 Limitation of Liability

- 4.1 You hereby acknowledge and agree that for all the links that may be contained on the Site and/ or content, your use of each web site, web page and Service is also subject to the terms and conditions of such web site and/ or web page in addition to The Company's Terms and Conditions and this privacy Policy, if any, contained within each website or web page or attached to any products or Services.
- 4.2 The Company shall under no circumstances assume any responsibility for and shall not endorse unless expressly stated, information and/content created or published by third parties that is included in the Site and the Services or which may be linked to and from the Site.
- 4.3 The Company hereby declares that it shall use its reasonable endeavors to ensure the maintenance and availability of the Site and the Services but claims no responsibility and/ or liability under no circumstances for the results of any defects that exist on the Site and/ or content.
- 4.4 Under no circumstances shall The Company be liable for damages including but not limited to any special, indirect, incidental, punitive or consequential damages or any damages whatsoever, whether in an action of contract, negligence, arising out of or in connection with the performance of or use of Services available on the Site and in particular, but without limitation to the foregoing, The Company specifically excludes all liability whatsoever in respect of any loss arising as a result of:
- any loss of any Services or your content resulting from delays, non-deliveries, missed deliveries, or Services interruptions; and
 - defects that may exist or for any costs, loss of profits, loss of your content or consequential losses arising from your use of, or inability to use or access or a failure, suspension or withdrawal of all or part of the Site and the Services at any time.
- 4.5 Under no circumstances shall The Company be liable for the following:
- any viruses, bugs and/ or any other disabling features that may affect your access to or use of the Site and/ or your device.
 - any incompatibility between the Site and other web sites, Services, software and hardware.

- c. any delays or failures you may experience in initiating, conducting, or completing any transmissions or transactions in connection with the Site in an accurate or timely manner

5 Remedies

Your sole and exclusive remedy under this Policy is to discontinue using the Site and/ or the Services in case you do not agree with this Policy, or you are not satisfied with the Site and/ or Services, or you have any claims whatsoever against The Company in respect to the Site and/ or Services.

6 Indemnity By You

You hereby undertake to fully indemnify and to hold The Company harmless in respect of all losses, costs, actions, proceedings, claims, damages, expenses (including reasonable legal costs and expenses), or liabilities, whatsoever suffered or incurred directly or indirectly by The Company from and against any claim brought by a third party resulting from your breach or non-observance of any of this Policy and/ or the use of the Site and the Services or the provision of content to The Company by you and in consequence of such use of the Site and the Services or provision of content.

7 General

- 7.1 Amendment - The Company reserves the right to amend the Policy, including any charges associated with the use of the Site. You are responsible for regularly reviewing this Policy, and any additional terms posted on the Site. Your continued use of the Sites after the effective date of such amendments constitutes your acceptance of and agreement to such amendments.
- 7.2 Assignment - The Company may assign this Policy in whole or in part to any third party at its discretion. You hereby undertake that you will not assign, re-sell, sub-lease or in any other way transfer your rights or obligations under this Policy or part thereof.
- 7.3 Severability - This Policy is severable in that if any provision is determined to be illegal or unenforceable by any court of competent jurisdiction such provision shall be deemed to have been deleted without affecting the remaining provisions of this Policy.
- 7.4 Waiver - The Company's failure to exercise any particular right or provision of this Policy shall not

constitute a waiver of such right or provision unless acknowledged and agreed to by The Company in writing.

- 7.5 Governing Law and Jurisdiction - This Policy shall be governed by and construed in accordance with the laws of the Hashemite Kingdom of Jordan, and you hereby submit to the jurisdiction of the competent Courts of Amman/ Abdali.
- 7.6 Representations - You acknowledge and agree that in agreeing to this Policy you do not rely on, and shall have no remedy in respect of, any statement, representation, warranty or understanding (whether negligently or innocently made) of any person (whether party to this Policy or not) other than as expressly set out in this Policy as a warranty.
- 7.7 Force Majeure - The Company shall not be liable in respect of any breach of this Policy due to any cause beyond its reasonable control including but not limited to, Act of God, inclement weather, act or omission of Government or public telephone operators or other competent authority or other party for whom The Company is not responsible.
- 7.8 Termination, Access Restriction - The Company hereby reserves the right to terminate this Policy, or terminate or suspend your access to the Site and/ or Services at any time, with or without cause, with or without notice. Upon such termination or suspension, your right to use the Site and/ or Services will immediately cease.
- 7.9 Language - The Policy was drafted in two original counterparts both in the English and Arabic languages. In the case of contradiction between the two versions, the terms of the English version shall prevail.

Exhibit 4

http://www.orange.jo/en/index.php

orange

SKY FALCON "click here"

search Google™ Custom Search enhanced by Google

the web orange.jo

at home on mobility at office youth

free Samsung Wave

with 3G+ Unlimited monthly subscriptions

drive your business the way you want

win 7 Mercedes cars during the summer with Orange

3G+ your world moves with you

get what you want

email & communicate

user name

password

other mails

how to activate your email

help & support

- assistance
- most viewed
- payment methods
- my first steps with Orange
- report a problem

get more help








<p>news football & sports</p>  <p>Lebanese troops, Israeli officer killed in border clash ADAYSSEH, Lebanon (AFP) - Lebanese and Israeli troops traded deadly fire on their tense border in the worst clash since the 2006 war between the...</p> <p>read more</p> <p>Orange Jordan news RSS feed</p>	<p>weather Amman change high: 40 low 23 7 day forecast</p> <p>prayer time, anasheed, quran, du'a enter islamic</p>	<p>Orange World</p> <ul style="list-style-type: none"> dandanah missed call alert web to SMS info channels games <p>visit Orange world</p>
<p>mbc tv</p> <ul style="list-style-type: none"> ASI Bani Jan Joelle <p><i>exclusive</i> click here to see MBC tv</p>	 <p>save time and effort by paying your bills here; it's easy, fast and safe!</p> <p>fixed internet mobile</p>	<p>order online</p> <ul style="list-style-type: none"> fixed ADSL surf & talk TV <p>today I'm happy</p>
<p><i>first time ever in Jordan</i></p> <p>New tax inclusive pay as go cards from Orange mobile</p> 	<p>lifestyle</p> <p>laki fashion cooking</p> <p>more life style</p> 	<p>discover <small>new news</small></p> <ul style="list-style-type: none"> entertainment radio play 99.6 yellow pages white pages chat games horoscope cinema <p>more</p>
<p>jobs join orange family read more</p> 		<p>our social responsibility</p> 

Exhibit 5


<http://www.tarasol.jo/privacy-policy>

Back to our old website | [Contact Us](#) | [Client login](#) | [My Cart](#) | [Search](#)

 [Products](#) [Download](#) [Shop](#) [Pricing](#) [How it works](#)

[Expatriates Offer](#)

Call **Jordan** with your local fees
from any where in the world



[subscribe now](#)

[Tarasol Phone](#) **Security Privacy Policy**

How it Works?
[→ \(Read more\)](#)

Client Login

Username:

Password:

[Forgot password](#)

© 2010 Tarasol Telecom [About Us](#) · [Jobs](#) · [Latest News](#) · [Success Stories](#) · [FAQs](#) · [Security Privacy Policy](#)

Exhibit 6

<http://www.xol.jo/PrivacyPolicy.aspx>

The screenshot shows the XOL Jordan website's Privacy Policy page. The browser address bar displays <http://www.xol.jo>. The page features a navigation menu with links for Home, News, Products, Plans, Support, Careers, FAQ, About us, and Contact us. A search bar is located in the top right corner. The main content area is titled "PRIVACY POLICY" and includes the following sections:

- Collection of Information:** XOL Jordan shall collect personally identifiable information (PII) from customers when initiating service and in connection with the provision or marketing of products and services. XOL Jordan may also collect non-personally identifiable information from customers and visitors regarding usage of our services or our web site (Non-PII).
- Anti-Spyware Policy:** XOL Jordan believes that Spyware is a threat to consumer privacy and his experience online. Therefore, we forbid any XOL Jordan employee, agent, partner, affiliate or contractor from intentionally deploying or using Spyware (as defined in this policy) on behalf of XOL Jordan.
- Use of Information:** XOL Jordan will use PII (1) to market products and services to customers and visitors that XOL Jordan believes may be of interest to them, (2) to provide product and services requested by customers and visitors and (3) to enable its vendors and contractors to provide and assist XOL Jordan in the marketing and provision of such services and products to XOL Jordan, customers or visitors.
- CPNI:** In the course of providing services to you, we collect and maintain certain Customer Proprietary Network Information (CPNI). CPNI includes the types of services you currently purchase, related usage and billing information for those services.

On the left side of the page, there are several utility links: "Your bag is empty" (Total Balance: \$ 0.00), "Clients login" (Username and Password fields), "Call rates" (Destination Country: Jordan), and "Services" (Phone Numbers, Prepaid Calling Card, Refill Card).

Security

XOL Jordan has invested and deployed a wide variety of technology and security features to make reasonable efforts to ensure the privacy of information on its network. In addition, XOL Jordan has implemented operations guidelines to ensure customer and visitor privacy is safeguarded at every level of its organization. XOL Jordan will continue to revise policies and implement additional security features as new technologies become available. However, no system or service can give a 100% guaranty of security, especially a service that relies upon the public Internet. Therefore, you acknowledge the risk that third parties may gain unauthorized access to your information when using our services.

Communications



XOL Jordan will not read, listen to or disclose to any third parties private e-mail, conversations, or other communications that are transmitted using XOL Jordan services except as required to ensure proper operation of services or as otherwise authorized by law.

You should be aware that any PII which you voluntarily include and transmit through publicly accessible forums (i.e., such as chat rooms, blogs, instant messages) may be viewed and used by anyone with access to such forums. XOL Jordan is unable to control such uses of your PII, and by using such services you assume the risk that the PII provided by you may be viewed and used by third parties.

Account Information

Subject to certain security requirements, XOL Jordan will do its best to honor requests from customers for account information, for example, name, address, company, or billing information. The customer is responsible for ensuring that the information on file with XOL Jordan is current and accurate.

Children's Privacy Policy

XOL Jordan does not sell products or services for purchase by children. XOL Jordan does not knowingly solicit or collect PII from children or teenagers under the age of eighteen. If you believe that a minor has disclosed PII to XOL Jordan, please call us at  00962 6 4000399  or email us at admin@xol.io

XOL Jordan Spam Policy



XOL Jordan has no tolerance for spam. Spam complaints will be dealt with seriously and can result in losing XOL Jordan privileges.

Third Party Web Sites and Services

Our service may contain links to other web sites and services not maintained by XOL Jordan. In addition, other web sites and services may also reference or link to XOL Jordan. We encourage you to be aware when you leave our service, or surf the Internet, and to read the privacy statements of each and every web site and service that you visit. We do not endorse, screen or approve, and are not responsible for the privacy practices or the content of, such other web sites and services.

XOL Jordan does not assume any liability for third parties that have been provided with information as permitted by this Privacy Policy or who have collected information as permitted by this Privacy Policy (such as advertisers using third party cookies).

Opt-out Policy

If you do not want your PII used by XOL Jordan for any direct marketing purposes, then you may opt-out of such disclosures by calling us at  00962 6 4000399 . You can also email us with your opt out request at admin@xol.io, include your name and account number, and identify which contact method(s) (email, telephone, direct mail .. etc) from which you wish to opt out.

However, we are not responsible for removing your PII from the lists of any third party who has previously been provided your information in accordance with this policy. Since XOL Jordan must use a customer's PII in order to provide them with XOL Jordan services, customers cannot opt-out of all uses of their PII unless they cancel their service.

Changes to policy

We reserve the right, at our discretion, to change, modify, add, or remove portions from this policy at any time by posting such changes here. You should review this policy regularly for changes, and can easily see if changes have been made by checking the Effective Date below. However, if at any time in the future we plan to use PII in a way that differs from this policy, we will post such changes here and provide you the opportunity to opt-out of such differing uses. Your continued use following the posting of any changes to this policy means you accept such changes.

Contents

All contents published on XOL Jordan web site reflect the latest available information. There is a possibility that some of the content may be outdated and this is not due to negligence, but is out of our control. Only formal documents are considered to be official and reflect all XOL Jordan changes. XOL Jordan is not to be held liable in respect to the content on this site if used in sole discretion. XOL Jordan has full rights to change content without prior notice.

Terms of Service

For customers, this Privacy Policy is subject to the XOL Jordan Terms of Service or other agreements between you and XOL Jordan. If you are a customer, please refer to the Terms of Service or such other agreements regarding certain rights and limitations with respect to your use of XOL Jordan's services.

The Hashemite Kingdom of Jordan

Our service is maintained in the Hashemite Kingdom of Jordan. By using our services, you authorize the export of PII to Jordan and its storage and use as specified in this policy.

Questions

For common questions and answers regarding our privacy policy or to contact us [click here](#)

Effective Date


This Privacy Policy was last updated on February 11, 2008.

© Copyright XOL 2010. All rights reserved. | [PRIVACY POLICY](#)


Designed & Developed by [Softimpact](#)

Exhibit 7

<http://www.mec.com.jo/>



مؤسسة الشرق الأوسط للاتصالات
Middle East Communications Corporation



Login | News & Events | Contact Us | Site Map

Main Menu


- Home
- + About MEC Communication
- + Solutions
- + Professional Services
- Our Partners & Clients





Privacy Policy

Middle East Communication Corporation has created this privacy statement to demonstrate its firm commitment to privacy. The following discloses our information gathering and dissemination practices for this website.

This site contains links to other sites. MEC is not responsible for the privacy practices or the content of such sites. MEC has also established relationships with partners but such relationships are generally technical in nature, or content collaborations. If any partner has access to any information entered by users in our database, this fact shall be disclosed to the user upon initiating the registration process. Users who feel they do not wish their information to be shared by anyone other than MEC may then opt out of completing the registration.

Contacting MEC
If you have any questions about this privacy statement, the practices of this site, or your dealings with this site, you may contact:


330, King Abdullah II st.
Tel.  +962-6-5818899 / 5819800 Fax: +962-6-5828684
P.O.Box 144040 Amman - 11844 - Jordan
[E-mail:mec@mec.com.jo](mailto:mec@mec.com.jo)




Terms of Use | Privacy Policy

Exhibit 9

<http://www.aa-telecom.com/dev/privacy.php>

Login to Your Account

[Home](#) [Contact](#) [Services](#) [Products](#) [Downloads](#) [Support](#)



AAT ONLINE PRIVACY STATEMENT

AAT respects your privacy and is committed to protect information that you share with us. In General, you can browse through our website without giving us any information about yourself. When we do need your personal information to provide services that you request or when you choose to provide us with your personal information, this policy describes how we collect and use your personal information.

Information Collection

Personal information means any information that may be used to identify an individual, including, but not limited to, a first and last name, email address, a home, postal or other physical address, other contact information, title, birth date, gender, occupation, industry, personal interests, other information when needed to provide a service you requested.

When you browse our website, you do so anonymously, unless you have previously indicated that you wish AAT to remember your login and password. We don't automatically collect personal information, including your email address. We do log your IP address (the Internet address of your computer) to give us an idea of which part of our website you visit and how long you spend there. But we do not link your IP address to any personal information unless you have logged in to our website. Like many other commercial websites, the AAT website may use a standard technology called a "cookie" to collect information about how you use the site. Please go to "Cookies and Tracking Information" below for more information.

AAT collects personal information when you register with AAT for a AAT account, when you use certain AAT products or services, when you register to attend a seminar or participate in an online survey, when you ask to be included in an email or other mailing list, or you submit an entry for a sweepstakes or other promotions, or when you submit your personal information to AAT for any other reason. From time to time, AAT receives personal information from business partners and vendors. AAT only uses such information if it has been collected in accordance with acceptable privacy practices consistent with this Policy and applicable laws.

Access to certain AAT web pages require a login and a password. The use of those web pages, and the information or programs downloadable from those sites, may be governed by a written agreement between your employer and AAT . Unless you request deletion of your personal information as specified below, your personal information may be retained by AAT to verify compliance with the agreement, log software licenses granted, to track software downloaded from those pages, or track usage of other applications available on those pages.

Notice

When personal information is collected, we will inform you at the point of collection the purpose for the collection. AAT will not transfer your personal information to third parties without your consent, except under the limited conditions described under the discussion entitled "Information Sharing and Disclosure" below.

If you choose to provide us with your personal information, we may only transfer that information, within AAT or to AAT 's third party service providers with your permission. Upon receiving your permission, we may transfer your information across borders and from your country or jurisdiction to other countries or jurisdictions around the world.

We will always give you the opportunity to "opt out" of receiving direct marketing or market research information. This means we assume you have given us your consent to collect and use your information in accordance with this Policy unless you take affirmative action to indicate that you do not consent, for instance by clicking or checking the appropriate option or box at the point of collection. In some cases, when applicable, we will provide you with the opportunity to "opt in." This means we will require your affirmative action to indicate your consent before we use your information for purposes other than the purpose for which it was submitted.

Cookies and Tracking Technology

A cookie is a small data file that certain Web sites write to your hard drive when you visit them. A cookie file can contain information such as a user ID that the site uses to track the pages you've visited, but the only personal information a cookie can contain is information you supply yourself. A cookie can't read data off your hard disk or read cookie files created by other sites. Some parts of AAT's website use cookies to track user traffic patterns. We do this in order to determine the usefulness of our website information to our users and to see how effective our navigational structure is in helping users reach that information.

If you prefer not to receive cookies while browsing our website, you can set your browser to warn you before accepting cookies and refuse the cookie when your browser alerts you to its presence. You can also refuse all cookies by turning them off in your browser, although you may not be able to take full advantage of AAT's website if you do so. In particular, you may be required to accept cookies in order to complete certain actions on our website. You do not need to have cookies turned on, however, to use/navigate through many parts of our website, except access to certain of AAT's web pages may require a login and password.

How We Use Information Collected?

AAT uses information for several general purposes: to fulfill your requests for certain products and services, to personalize your experience on our website, to keep you up to date on the latest product announcements, software updates, special offers or other information we think you'd like to hear about either from us or from our business partners, and to better understand your needs and provide you with better services. We may also use your information to send you, or to have our business partners send you, direct marketing information or contact you for market research.

Information Sharing and Disclosure

Because AAT is a global company, your personal information may be shared with other AAT offices or subsidiaries around the world. All such entities are governed by this Privacy Policy or are bound by the appropriate confidentiality and data transfer agreements.

Your personal information is never shared outside AAT without your permission, except under conditions explained below. Inside AAT, data is stored in controlled servers with limited access. Your information may be stored and processed in the United States or any other country where AAT, its subsidiaries, affiliates or agents are located.

AAT may send your personal information to other companies or people under any of the following circumstances: when we have your consent to share the information; we need to share your information to provide the product or service you have requested; we need to send the information to companies who work on behalf of AAT to provide a product or service to you (we will only provide those companies the information they need to deliver the service, and they are prohibited from using that information for any other purpose); or we want to keep you up to date on the latest product announcements, software updates, special offers or other information we think you'd like to hear about either from us or from our business partners (unless you have opted out of these types of communications). We will also disclose your personal information if required to do so by law, to enforce our Terms, or in urgent circumstances, to protect personal safety, the public or our websites.

Your Ability to Review and Delete Your Account and Information

You may request deletion of your AAT account or any of your personal information held by us.

Data Security

Your AAT account information is password-protected for your privacy and security. AAT safeguards the security of the data you send us with physical, electronic, and managerial procedures. While we strive to protect your personal information, we cannot ensure the security of the information you transmit to us, and so we urge you to take every precaution to protect your personal data when you are on the Internet. Change your passwords often, use a combination of letters and numbers, and make sure you use a secure browser.

Children and Privacy

Our websites do not target and are not intended to attract children under the age of 18. AAT does not knowingly solicit personal information from children under the age of 18 or send them requests for personal information.

Third Party Sites

AAT's website contains links to other sites. AAT does not share your personal information with those websites and is not responsible for their privacy practices. We encourage you to learn about the privacy policies of those companies.

Our website may contain links to websites operated by other companies. Some of these third-party sites may be co-branded with a AAT logo, even though they are not operated or maintained by AAT. Although we choose our business partners carefully, AAT is not responsible for the privacy practices of web sites operated by third parties that are linked to our site. Once you have left our website, you should check the applicable privacy policy of the third party website to determine how they will handle any information they collect from you.

Changes to this Privacy Policy

AAT will amend this policy from time to time. If we make any substantial changes in the way we use your personal information we will make that information available by posting a notice on this site.

Questions or Suggestions

If you have questions or concerns about our collection, use, or disclosure of your personal information, please email us at info@aa-telecom.com.

Appendix C

Exhibits 1-20

Exhibit 1

<http://www.arabbank.com.jo/en/privacypolicy.aspx>



Privacy Policy

We Value Your Privacy

Your privacy and security is very important to us. At Arab Bank, we treat your personal information as private and confidential. We are dedicated to protecting your privacy and providing you with the highest level of security. This statement describes what personal information we collect, what we do with it, and how we protect it.

Security of Your Personal Information

We take appropriate measures to keep your personal information, that we hold about you, secure and ensure that it is protected from loss, unauthorized access, misuse, modification, or disclosure. Your personal information with us remains secure because of:

- The strict security measures and technologies we use to prevent fraud and to protect our systems from intrusion.
- Security controls and processes that are updated regularly to meet or exceed industry standards.
- Our employees are trained to respect the confidentiality of any personal information held by us.

Protecting Your Privacy

To help you in protecting your personal information, we recommend the following:

- Regularly check your account balance and bank statements and report promptly any discrepancies to your branch.
- Contact us immediately if you believe someone else may have access to your password, user ID, PIN, or other confidential information.
- Do not share confidential information via the telephone or online unless you know or can verify the recipient.
- Ensure that your account records are properly disposed.
- Utilize a secure browser when conducting transactions online, close online applications when not in use, and ensure virus protection is regularly updated.

For more information on how to protect your password security and other related practices designed to safeguard the privacy and security of your financial information, please visit our [Security Statement](#).

What Information We Collect and Use

We collect and use information about you to administer our business and provide you with high quality financial products and services. We collect information about you from a variety of sources, such as:

- Applications, personal financial statements, and other written or electronic communications reflecting information such as your name, address, identification number, occupation, assets, and income.
- Transactional account history including your account balance, payment records, and credit card usage.
- Information received from third parties, (e.g. government, regulatory, or credit agencies).

How We Use Your Information

Any personal information provided by you to Arab Bank will be used for the purpose of providing and operating the products and services you have requested and for other related purposes which may include, updating and enhancing Arab Bank records, understanding your financial needs, conducting credit checks, reviewing credit or loan eligibility, advising you of other products and services that may be of interest to you, for fraud prevention, debt collection purposes, and for purposes required by law or regulation.

Sending E-mails to Arab Bank

When inquiring or requesting information about a specific product or service, or in case of volunteering information using any of Arab Bank's contacts, (e.g. General Inquiry form) we will use your e-mail address to reply, and we may store your e-mail address, your message, and our response for quality assurance purposes. We may also do this to meet our legal and regulatory requirements.

Who We Share Information With

We may share the information about you and your dealings with us, to the extent allowed by law, with:

- Arab Bank Branches and Subsidiaries;
- Regulators;
- External Auditors;
- Third party service providers;
- Agents acting on behalf of Arab Bank.
- Arab Bank staff as well as third parties with permitted access to your information are required to observe our confidentiality obligations.

Maintaining Accurate Information

Keeping your account information accurate and up to date is very important. You have access to your account information, which includes your contact information, account balances and transactions, and similar information, through various means, such as account statements, Phone Banking, and Internet Banking. If you discover inaccuracies in your personal information, please promptly notify the branch or office where you do business, so that we can make the necessary updates or changes.

Changes to This Statement

From time to time, it may be necessary for us to amend our Privacy Statement. The current version will be maintained on our Website.

Changes to This Statement

From time to time, it may be necessary for us to amend our Privacy Statement. The current version will be maintained on our Website.

Exhibit 2


<http://www.ahli.com/>

Jordan | [Cyprus](#) | [Lebanon](#) | [Palestine](#) [العربية](#) | [Contact Us](#)

ahli | الأهلي البنك الأهلي الأردني
Jordan Ahli Bank

Home | [About Ahli Bank](#) | [Ahli Services](#) | [Investors Corner](#) | [Careers](#) | [Online Banking](#) | [Feedback](#) [GO](#)

[PERSONAL](#)
[MY BUSINESS](#)
[CORPORATE](#)
[PREMIUM](#)
[INVESTMENT](#)
[CAPITAL](#)
[BANCASSURANCE](#)
[FINANCIAL LEASING](#)



Other Services

- [Site Map](#)
- [Ahli Bank's Reports](#)
- [Ahli Branches & ATM Locator](#)
- [My Portfolio](#)
- [Saving Accounts Winners](#)
- [Inquiry Form](#)
- [FAQ's](#)
- [Secure Code](#)
- [Ahli Bank TV Commercials](#)
- [Ahli Bank's Museum](#)
- [Loan Calculators](#) **New**

Latest News

- [Jordan Ahli Bank participates as a Silver Sponsor at the Sixth Jordanian Businessmen and Investors Conference](#)
The Development Zones Commission (DZC) announced its participation as a Silver Sponsor in the Sixth Jordanian Businessmen ..
- [Jordan Ahli Bank Organizes a Field Visit for the Children of the Orphan Care Society](#)
Leading financial institution Jordan Ahli Bank organized a visit to the Children's Museum ..
- [Jordan Ahli Bank Inaugurates the Ahli Financial Leasing Company](#)
In its longstanding commitment to provide a comprehensive lineup of quality banking services ..

[More](#)

Your comments , ideas are valuable to us

Exhibit 3

<http://www.cab.jo>

Home Online Banking Our Services CAB News About CAB Contact CAB Investor Relations Iris Recognition

بنك القاهرة عمان
CairoAmmanBank

CAB Online Survey

All rights reserved in compliance with the Jordanian unfair competition law, agreements, international standards and all effective laws.

Delivering Growth

Legal Information | Accessibility | Security and Privacy | Site map | Cab Estate | Awraq

Developed By Batelco Jordan

Exhibit 4

<http://bankofjordan.com/boj50en/inside.htm?id=8&src=instruction>



The header of the Bank of Jordan website features a dark blue navigation bar with the bank's logo and name in Arabic (بنك الأردن) and English (Bank of Jordan). To the right, there are icons for home, mobile, chat, globe, and search, along with a search input field and a 'Website'/'Internet' toggle. Below the navigation bar, there is a section titled 'Excel' with a collage of business-related images and a list of services: Retail Services, Corporate Services, SMEs, Leasing Services, and Investment Services. The word 'عربي' (Arabic) is visible in the top right corner.

Privacy Policy

Bank of Jordan is highly concerned with information safety, security and protection and exerts extensive efforts to take all effective security measures and procedures in order to ensure safety of information. These measures include; continuously reviewing security measures and periodically checking security violations, yet these efforts will not be fruitful without clients' understanding and commitment to the concept of information security.

Thus, kindly read and comprehend the following Privacy Policy and Terms of Use periodically and before browsing our website.

1. Clients may visit Bank of Jordan's website without disclosing any personal information.
2. In case clients provided the Bank with any personal information such as: names, addresses or e-mails which may be necessary for mutual correspondence and communication; Bank of Jordan will be obliged to keep such information secure and not to disclose such to any third party in accordance with the effective Laws.
3. Clients shall provide the bank with a means of communication and shall periodically update their information if changed, to enable the bank to contact them in cases of emergency.
4. Clients shall not send any personal information or their bank account information through e-mail; as it is not a safe method of dispatching personal information.
5. Clients should ensure signing out after using internet-banking services.
6. The system will automatically sign out the client after a while, in case the internet-banking window is left open without being used.
7. E-Linking to other Websites:
Banks offering internet-banking services are targeted sites for linking; the common means of which are emails and fake sites that ask users for sensitive information such as information of Identification Cards, Passwords, Account Information and Credit Card Information.
Thus, clients should be alert regarding these linking attempts by ensuring signing in to Bank of Jordan's official website (www.bankofjordan.com) before disclosing any information, as there are some hackers who design fake sites that look like the original websites but with small spelling differences.
8. Password:
Kindly keep your login password secure, change it periodically, and do not disclose it to any third party including the bank employees.

9. Viruses:

Kindly make sure to install and activate a recent virus scanning software on your PC.

10. Intellectual Property Rights:

No information displayed on the Bank's Website can be used or disseminated without the bank's previous written consent.

11. Limited Liability:

Browsing/using Bank of Jordan's website will be on the user's personal responsibility, as Bank of Jordan will not be responsible for any claims, losses, costs, expenses or compensations of any kind, without any private or public limitations, regarding the use of its website and the information displayed on the site.

12. Guarantees:

Bank of Jordan's website on the internet may include some information from other parties subscribed to the internet. Thus, Bank of Jordan does not offer any implicit or explicit guarantees regarding any information offered by third parties or through any link to other websites on the internet. Also, Bank of Jordan bears no responsibility regarding the preciseness and credibility of information, software, offers or activities offered by any third party, websites or links that may be linked to its website.

13. Security of Information:

Bank of Jordan uses a set of techniques to protect saved information against loss, misuse, unauthorized access, unauthorized disclosure, change or deletion.

14. Reporting Security Violations:

If you are in doubt of any security violation of your e-account/e-accounts, or if any transaction was executed by any other unauthorized party; you should immediately report such violation to Bank of Jordan via the following email: boj@bankofjordan.com.jo or by calling +962 6 5696277 extension 2487.

15. Bank of Jordan has the right to change or amend these terms and conditions, any other content or part of its website at any time, without dispatching any previous notice. Your entry to Bank of Jordan's website shall be regulated by the effective terms and conditions at that time.

Exhibit 5

<http://www.hbtf.com/wps/portal>

بنك الإسكان للتجارة والتمويل
The Housing Bank for Trade & Finance

About Us | Investor's Relations | FAQ's | Branches Network | Contact Us | Site Map | Log In

عربي

Home | Retail Banking | Commercial Banking | Treasury & Investment | Financial Institutions | Internet Banking

Terms & Conditions Of Use

Please read these terms and conditions carefully.

By accessing this site and any pages thereof, you agree to be bound by the terms and conditions below. If you do not agree to the terms and conditions below, do not access this site, or any pages thereof.

copyright © the housing bank for trade & finance 2002 . All rights reserved

Copyright in the pages and in the screens displaying the pages, and in the information and material therein and in their arrangement, is owned by the housing bank for trade & finance (here in after referred to as " the housing bank ") , unless otherwise indicated .

Use of information and materials :

The information and materials contained in this site - and the terms, conditions and descriptions that appear - are subject to change without notice. Nothing in this site shall be construed as an offer to engage in any transaction, nor does it constitute an investment, legal, tax or other advice, nor is to be relied upon in making an investment or other decisions. You should obtain relevant and specific professional advice before making any investment decision. Your eligibility for particular products or services is subject to final determination and acceptance of the housing bank .

Unauthorized use of the housing bank's web sites and systems including but not limited to an authorized entry into the housing bank's systems misuse of passwords , or misuse of any information posted on a site is strictly prohibited .

No warranty :

The information and materials contained in this site, including text , graphics, links or other items are provided "as is", "as available" the housing bank does not warrant the accuracy, adequacy or completeness disclaims liability for errors or omissions in this information and materials. No warranty of any kind, implied expressed or statutory, including but not limited to the warranties of non-infringement of third party rights, title, merchantability, fitness for a particular purpose and freedom from computer virus, is given in conjunction with the information and materials.

Limitation of liability:

In no event will the housing bank be liable for any damages, including without limitation direct or indirect, special, incidental, or consequential damages, losses or expenses arising in connection with this site or use thereof or inability to use by any party, or in connection with any failure of performance, error, omission, interruption, defect, delay in operation or transmission, computer virus or line or system failure, even if the housing bank , or representatives thereof, are advised of the possibility of such damages, losses or expenses. This site may contain links to web sites of third parties .the housing bank hereby disclaims liability for any information , materials , products or services posted or offered at any of the third party sites linked to this web site .

The content, accuracy, opinions expressed, and other links provided by these resources are not investigated, verified, monitored, or endorsed by the housing bank .

Submissions:

All information submitted to the housing bank via this site shall be deemed and remain the property of the housing bank and the housing bank shall be free to use, for any purpose, any ideas, concepts, know how or techniques contained in information a visitor to this site provides the housing bank through this site. The housing bank shall not be subject to any obligations of confidentiality regarding submitted information except as agreed by the housing bank entity having the direct customer relationship or as otherwise specifically agreed or required by law.

Additional terms :

Certain sections or pages on this site may contain separate terms and conditions , which are in addition to these terms and conditions . In the event of a conflict , the additional terms and conditions will govern for those sections or pages .

Governing law :

Use of this site shall be governed by all applicable laws of the hashimite kingdom of jordan including the law of electronic transaction no. (85) of (2001) .

Exhibit 6

<http://www.jordan-kuwait-bank.com/en/terms.html>



Terms & Conditions

JORDAN KUWAIT BANK'S WEB SITE

Introduction:

- BY ACCESSING THIS SITE AND ANY PAGES THEREOF, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS BELOW.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS BELOW, DO NOT ACCESS THIS SITE, OR ANY PAGES THEREOF.

- CERTAIN SECTIONS OR PAGES ON THIS SITE MAY CONTAIN SEPARATE TERMS AND CONDITIONS , WHICH ARE IN ADDITION TO THESE TERMS AND CONDITIONS . IN THE EVENT OF A CONFLICT , THE ADDITIONAL TERMS AND CONDITIONS WILL GOVERN FOR THOSE SECTIONS OR PAGES .

COPYRIGHT ©

COPYRIGHT © JORDAN KUWAIT BANK ALL RIGHTS RESERVED

- Copyright in the pages and in the screens displaying the pages, and in the information and material therein and in their arrangement, are the property of JORDAN KUWAIT BANK.

- ALL INFORMATION SUBMITTED TO JORDAN KUWAIT BANK VIA THIS SITE SHALL BE DEEMED AND REMAIN THE PROPERTY OF JORDAN KUWAIT BANK AND JORDAN KUWAIT BANK SHALL BE FREE TO USE, FOR ANY PURPOSE, ANY IDEAS, CONCEPTS, KNOW HOW OR TECHNIQUES CONTAINED IN INFORMATION A VISITOR TO THIS SITE PROVIDES JORDAN KUWAIT BANK THROUGH THIS SITE. JORDAN KUWAIT BANK SHALL NOT BE SUBJECT TO ANY OBLIGATIONS OF CONFIDENTIALITY REGARDING SUBMITTED INFORMATION EXCEPT AS AGREED BY JORDAN KUWAIT BANK ENTITY HAVING THE DIRECT CUSTOMER RELATIONSHIP OR AS OTHERWISE SPECIFICALLY AGREED OR REQUIRED BY LAW.

USE OF INFORMATION AND MATERIALS

-THE INFORMATION AND MATERIALS CONTAINED IN THIS SITE – AND THE TERMS, CONDITIONS AND DESCRIPTIONS THAT APPEAR - ARE SUBJECT TO CHANGE WITHOUT NOTICE.

- NOTHING IN THIS SITE SHALL BE CONSTRUED AS AN OFFER TO ENGAGE IN ANY TRANSACTION, NOR DOES IT CONSTITUTE AN INVESTMENT, LEGAL, TAX OR OTHER ADVICE, NOR IS TO BE RELIED UPON IN MAKING AN INVESTMENT OR OTHER DECISIONS. YOU SHOULD OBTAIN RELEVANT AND SPECIFIC PROFESSIONAL ADVICE BEFORE MAKING ANY INVESTMENT DECISION. YOUR ELIGIBILITY FOR PARTICULAR PRODUCTS OR SERVICES IS SUBJECT TO FINAL DETERMINATION AND ACCEPTANCE OF JORDAN KUWAIT BANK .

NO WARRANTY

THE INFORMATION AND MATERIALS CONTAINED IN THIS SITE, INCLUDING TEXT , GRAPHICS, LINKS OR OTHER ITEMS ARE PROVIDED "AS IS", "AS AVAILABLE" JORDAN KUWAIT BANK DOES NOT WARRANT THE ACCURACY, ADEQUACY OR COMPLETENESS DISCLAIMS LIABILITY FOR ERRORS OR OMISSIONS IN THIS INFORMATION AND MATERIALS. NO WARRANTY OF ANY KIND, IMPLIED EXPRESSED OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM COMPUTER VIRUS, IS GIVEN IN CONJUNCTION WITH THE INFORMATION AND MATERIALS.

LIMITATION OF LIABILITY:

IN NO EVENT WILL JORDAN KUWAIT BANK BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION DIRECT OR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSSES OR EXPENSES ARISING IN CONNECTION WITH THIS SITE OR USE THEREOF OR INABILITY TO USE BY ANY PARTY, OR IN CONNECTION WITH ANY FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION, DEFECT, DELAY IN OPERATION OR TRANSMISSION, COMPUTER VIRUS OR LINE OR SYSTEM FAILURE, EVEN IF JORDAN KUWAIT BANK , OR REPRESENTATIVES THEREOF, ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. THIS SITE MAY CONTAIN LINKS TO WEB SITES OF THIRD PARTIES . JORDAN KUWAIT BANK HEREBY DISCLAIMS LIABILITY FOR ANY INFORMATION , MATERIALS , PRODUCTS OR SERVICES POSTED OR OFFERED AT ANY OF THE THIRD PARYT SITES LINKED TO THIS WEB SITE .

THE CONTENT, ACCURACY, OPINIONS EXPRESSED, AND OTHER LINKS PROVIDED BY THESE RESOURCES ARE NOT INVESTIGATED, VERIFIED, MONITORED, OR ENDORSED BY THE BANK .

GOVERNING LAW :

USE OF THIS SITE SHALL BE GOVERNED BY ALL APPLICABLE LAWS OF THE HASHIMITE KINGDOM OF JORDAN INCLUDING THE LAW OF ELECTRONIC TRANSACTION NO. (85) OF (2001) .

[Home](#) | [About Us](#) | [Products & Services](#) | [Treasury & Markets](#) | [Branch Network](#) | [Financial](#) | [JKB Publications](#) | [Annual Report](#) | [Investors Relations](#) | [News](#) | [Links](#) | [Contact us](#) | [Inquiry Form](#) | [Mailing List](#) | [Apply for a Loan](#) | [Loan calculator](#) | [Net Banker](#) | [Webmail](#) | [Site Map](#)

Copyright © 2006 Jordan Kuwait Bank :: [Terms & Conditions](#)

Designed & Maintained By [Access to Arabia](#)

Exhibit 7

<http://www.ajib.com/>

بنك الاستثمار العربي الأردني
ARAB JORDAN INVESTMENT BANK

AJIB

Home | Products & services | Branches | Feedback | Site map | Contact us | عربي

Search GO

- About us
- Annual Reports
- AJIB Group
- Main Services
- Investment Banking Services
- Corporate Banking Services
- Retail Banking Services
- Research Banking Services
- Quick links
- Correspondent Banks

Welcome to AJIB

The Arab Jordan Investment Bank (AJIB) is Jordan's leading investment and private bank. AJIB offers a wide variety of investment, commercial and private banking products and solutions tailor-made to suit the requirements of our discerning clientele. AJIB continues to leverage its resources; technology and banking best practices to meet and exceed the ever growing needs of corporate, high net-worth individuals and sophisticated clients in Jordan and the region.

Over the past thirty two years, AJIB grew to become a major player in the region's investment banking scene, providing its clients with corporate finance services including mergers and acquisitions, equity capital markets (IPOs and secondary offerings), transaction advisory services, project finance and equity research.

AJIB serves clients through 25 branches and offices covering major locations in Jordan, assisted with an advanced network of 20 ATMs distributed throughout the Kingdom. The Bank has expanded to provide services outside Jordan through its branch in Limasol-Cyprus, as well as a representative office in Tripoli-Libya. In 2006 the Bank established Arab Jordan Investment Bank (Qatar) L.L.C. in the Qatar Financial Center to serve our clients in Qatar and the Gulf region. The United Arab Jordan Company for Investment and Financial Brokerage is a subsidiary of the Bank dedicated to serving our clients investment needs at the Amman Stock Exchange. Arab Advisors Group, the Bank's research subsidiary, is the recognized regional leader in research in the fields of finance, telecom, IT, and media. Its research offerings are highly regarded by the region's leading professionals.

[More...](#)

AJIB News

AJIB Operates its New, Fully-Integrated Core Banking System

The AJIB 2010 retail advertising campaign includes great packages

رغم الشبكات القوي التكنولوجي
من خلال فريق العمل
الذي يخدمنا
بمزيد من الكفاءة
والسرعة
في تقديم الخدمات
التي نقدمها
لعملائنا

Call Free 0800 22 026
Or Call (06) 5607126
Ext 345, 533, 567

Branches & Subsidiaries

- Local Branches & Offices
- International Branches & Offices
- Subsidiaries
- ATM Locations

Cyprus, Jordan

Online Banking \ Jordan
7 Open days a week 24 hours a day

Login

**Arab Jordan
Investment Bank
Qatar (L.L.C.)**



Online Banking \ Qatar

Login

Investment & Private Banking

At AJIB we provide advisory services to help private investors and corporations locate and acquire investment opportunities that match specific clients objectives.

By forging long-term partnerships and drawing on the expertise of our industry, country and product specialists, we succeed in meeting our clients' aspirations in a challenging global environment.

[More...](#)

Retail Banking Services & Visa Credit Cards

- [Housing Loans](#)
- [Personal Loans](#)
- [AJIB Visa Credit Cards](#)
- [Car Loans](#)

[More...](#)

Online Visa Applications









ARAB
ADVISORS
GROUP

A Member of the
Arab Jordan Investment Bank Group

Developed By Batelco Jordan

Exhibit 8

www.jordanislamicbank.com

Jordan Islamic Bank
Partners in achievement...

"Allah has permitted trade & forbidden usury."

Internet Banking

Jordan Islamic Bank About Us Accounts Financing & Advisory Services Banking Services Site Map Contact Us Search

Electronic Services
Internet Banking Services
SMS Services
Our Banking Services
Requests
Other Services
Find our ATMs Branches

Quick Contact
Jordan Islamic Bank

Terms & Conditions

Member of Al baraka Banking Group

Lease ending in ownership

1 2 3 4

Latest News View All News
- JIB honors pioneers of scouts and guides in Arab World...
more

Calendar

S	M	T	W	T	F	S
					1	2 3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Currency Converter
Jordan Dinars (JOD) 1.00
EURO (EUR)

Pray Time / Amman
Esha 9:00 | Maghreb 7:30 | Aser 4:23 | Dehor 12:42 | Fajer 4:22

Weather / Amman

Today's Prayer
اللهم إنا نسألك خبزنا من الغيب و

Craftsmen Financing My Needs Financing My House Financing My Car Financing

© 2010, JIB. All rights reserved. Designed by Creativitydesign

Exhibit 9

<http://www.jifbank.com/>



[Home](#)

[عربي](#)



[About us](#) | [Services](#) | [Publications](#) | [Careers](#) | [Contact us](#)

IN 0.62 AEIV 0.73 AFIN 2.85 AGICC 0.88 AIEI 2.35 AJIB 1.28 AMAL 1.16 Index 2265.4 Market Closed 1.01%



Real Estate For Sale

Statement by the Chairman

Controlling the Money Supply...
The Central Bank of Jordan exercised its role in steering the monetary policy by being vigilant and cautious. This has mitigated the severity of the global crisis on the financial system and contributed towards containing the consequent adverse ramifications.

Performing Under Pressure...
In this context, the growth achieved by the bank during 2008 is a testament to the healthy performance delivered under pressure and our ability to continue the journey on the same positive path. The bank is no stranger to this. Since its inception in 1982, our bank was able to overcome all challenges and reinforce its position – what position is it reinforcing?! - in the marketplace.

Sustainable Banking Relationships...
Our bank maintained its prudence in the provision of its banking services to its customers; be those corporations, SME, or retail. Our aim is to cultivate sustainable banking relationships with our customers, by focusing on a client base that is characterized by being loyal to the bank, coupled with qualified and proactive human capital who are the providers of our banking service



Online Banking

[Login](#) [الدخول](#)



Forbes.com
Business News and Financial News at Forbes.com

Recent Posts

Secrets Of Engaging Customers In Online Communities
Keep groups small, relevant, transparent.

employees

- Investbank wishes all its stakeholders a Happy Eid
- Products and services to be launched soon

Quick Links



Brokernet

[Log in](#) [الدخول](#)

بروكرنت



NetApp's Social Culture
Why telecommuting is not a priority for the Silicon Valley firm.

[Get Widget](#)

A secure way to shop online
طريقة آمنة للتسوق عبر الانترنت

All Copyrights Reserved for Investbank, 2008®

Exhibit 10

<http://www.arabbanking.com/En/Pages/LegalNotice.aspx>



Legal Notice

Important Legal Notice

Please read this legal notice carefully. If you continue to use this website (and that expression includes each of its pages as well as the content of those pages and (where relevant) the arrangement of that content), you agree to the terms of use in this notice. If you do not agree to be bound by this notice, please exit this website immediately. Certain sections of this website or other websites accessed through it may contain separate terms of use, which are in addition to this notice. Users should read those separate terms carefully. If they conflict with this notice, those separate terms will govern access to and use of those sections and websites.

Access

Arab Banking Corporation (B.S.C.) ("ABC") has made the information on this website available as a service to its customers and others for general information only. This website is not intended for persons located or resident in jurisdictions which restrict the distribution of the content of (or content of the kind on) this website. When accessing this website, persons are required to inform themselves about and observe any relevant restrictions. The host server for this website is located in a secure host data centre.

Use

Unless otherwise specified this website is for personal use only. Unauthorized use of the website is strictly prohibited. Permission is given for the downloading and temporary storage of one or more pages of the website for the purpose of viewing on a personal computer or monitor. The reproduction, permanent storage or retransmission of any content of this website is prohibited without the prior written consent of ABC.

Links

This website may contain links to websites controlled by third parties that are not ABC affiliates. Except as otherwise indicated ABC does not sponsor, endorse, recommend or approve the contents of any such websites and accepts no responsibility for information provided on any such websites by independent providers. Such third parties may have different privacy policies from ABC and third party websites may provide less security than the ABC website.

Changes

ABC reserves the right, in its sole discretion, without any obligation and without notice, to change, improve or correct the content of this website and to suspend and/or deny access to it. Any dated information is published as of its date only, and ABC does not undertake any obligation to update or amend any such information. ABC may discontinue or change any product or service described in this website, without notice, at any time.

No Warranty

Whilst ABC endeavours to ensure that the content of this website is current, correct and complete, the website is provided "as is" and no warranty, express or implied, is given as to its currency, accuracy, adequacy or completeness or that any indicated returns will be achieved. To the fullest extent permitted by applicable law, ABC disclaims any and all express or implied warranties and conditions including, without limitation, warranties and conditions as to merchantability and fitness for a particular purpose, title and non-infringement of third party rights. ABC does not warrant that this website and any content (including any third party content) will be uninterrupted or error free, that defects will be corrected or that this website, the servers from which it is made available or any connected website are free of viruses or other harmful components.

Limitation Of Liability

Access to and/or use of this website is at the user's own risk. Users assume full responsibility and risk of loss resulting from access to and/or use of this website. ABC is not liable for loss or damage of any kind whatsoever arising as a result of (i) content on this website, including third party content, computer viruses and other harmful components; (ii) any errors in or omissions from this website; or (iii) access to and/or use of or inability to access and/or use this website for any reason. To the fullest extent permitted by applicable law, ABC excludes liability for any loss of profits or revenue, loss of business or goodwill, loss of or damage to data or direct, indirect, consequential, special or incidental loss arising from access to and/or use of or inability to access and/or use this website, even if advised of the possibility of such loss or damage or if such loss or damage was foreseeable. Nothing in this notice excludes or limits ABC's liability for fraud or for personal injury or death caused by ABC's negligence.

No Solicitation Or Advice

Except as otherwise specifically agreed in writing or as provided in any other applicable terms (i) nothing on this website is an offer which can be accepted so as to create contractual obligations without further action by ABC; (ii) ABC provides no advice with respect to the use of the website (including, without limitation, regarding the execution of transactions or any legal, tax or accounting advice or advice regarding the suitability or profitability of a security, investment or transaction by means of the website); and (iii) the website is not intended as financial advice or as an offer, solicitation or recommendation of securities or other financial products.

Users should obtain independent financial advice that addresses their particular investment objectives, financial situation and needs before making investment decisions. ABC, its affiliates and their respective officers, directors and employees may, from time to time, own or hold positions in or act as market makers or act as advisors, brokers or commercial and/or investment bankers in respect of any financial instruments (including related derivative contracts) discussed on this website. Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by ABC and/or its affiliates.

Intellectual Property Rights

This website and its arrangement are property protected by copyright, database rights and other intellectual property rights. ABC and, where appropriate, its third party suppliers retain all right, title and interest in and to that property. Use of the website does not confer any ownership rights in that property.

Tracking software

This website may use tracking software such as "cookies" to generate personal identification data for users. This function is designed to personalise website viewing and may enhance use. Your browser's options or preferences menu may offer notification and/or disablement of such software.

Group Information

Arab Banking Corporation (B.S.C.) is a Joint Stock Company established in the Kingdom of Bahrain pursuant to Amiri Decree Law No. 2 of 17 January, 1980 and registered in the Commercial Register under C.R. No. 10299, with an authorised share capital of one thousand five hundred million United States dollars (US\$2,500,000,000), a fully subscribed and paid up share capital of one billion United States dollars (US\$2,000,000,000) and its head office at ABC Tower, Diplomatic Area, PO Box 5698, Manama, Bahrain. It is licensed as an Offshore Banking Unit by the Bahrain Monetary Agency and listed on the Stock Exchanges of Bahrain (with effect from 7 May 1990) and Paris (with effect from 25 June 1990).

The ABC Group includes foreign banks, securities companies and financial institutions licensed by regulators in their countries of incorporation.

The services described in the website are provided by ABC or its subsidiaries and/or affiliates in accordance with appropriate local legislation and regulation.

Submissions

All submissions to ABC via this website (including all ideas, concepts, know-how or techniques contained in them) shall be and remain ABC property. ABC shall be free to use, for any purpose, any such submission and shall not be subject to any obligations of confidentiality regarding it except as agreed in writing or required by law. However, this does not limit or reduce ABC's obligations to customers in accordance with the privacy policy in this notice.

Privacy

ABC may collect, use and disclose personal data about users of its website so that it can carry out any obligations owed to users and for other related purposes, including monitoring and analysis of its business, crime prevention, legal and regulatory compliance, the marketing by ABC of other services and transfer of any of ABC's applicable rights or obligations. ABC will not disclose any personal data it collects about users to third parties except: (i) to the extent that it is required to do so by any applicable law or regulation; (ii) where there is a duty to the public to disclose; (iii) where ABC's interests require disclosure; or (iv) at a user's request or with a user's consent.

ABC may disclose personal data about users to those who provide services to ABC or act as ABC's agents, to any person to whom ABC transfers or proposes to transfer any of its applicable rights or obligations and to licensed credit reference agencies or other organisations that help ABC and others make credit decisions and reduce the incidence of fraud or in the course of carrying out identity, fraud prevention or credit control checks. ABC may also transfer information collected and held about users to any country, including countries without data protection laws, for any of the purposes described in this part.

Users may have a right of access to some or all of the personal data ABC collects and holds about them, or to have inaccurate information corrected, under applicable data protection laws. Any user wishing to exercise such rights should contact ABC in writing.

Governing Law

The above terms of use are governed by the laws of the Kingdom of Bahrain.

[Legal Note](#) | 2010 Arab Banking Corporation (B.S.C.). All rights reserved.

Exhibit 11

<http://www.unionbankjo.com/>

The screenshot shows the Union Bank website homepage. At the top, the bank's name is written in Arabic "بنك الإتحاد" and English "Union Bank" next to a pyramid logo. Navigation links for Home, Sitemap, and Contact Us are in the top right. A search bar is on the left. A central banner for "Housing Loan" features a house on clouds with a ladder, with the tagline "Making Your Dream Home a Reality". To the right, there are sections for "Corporate Banking" and "Personal Banking" with images of people and a cash machine. Below the housing loan banner is a "LOAN CALCULATOR" and "ANNUAL REPORTS" section. A "OUR LATEST NEWS" section lists recent events. At the bottom right, there is a "فلوسك بحسابك عطول!" (Your money is exhausted from your account!) promotion. The footer contains the copyright notice: © 2010 Developed by dot.jo. All rights reserved.

بنك الإتحاد
Union Bank

Home Sitemap Contact Us

Search

Services Inquiry form Real State for Sale

Housing Loan

Making Your Dream Home a Reality

Corporate Banking

Personal Banking

الإيداع النقدي الفوري
عن طريق جهاز الصراف الآلي

فلوسك
بحسابك عطول!

LOAN CALCULATOR

ANNUAL REPORTS

- Annual Report 2009 (English)
- Annual Report 2009 (Arabic)

More...

OUR LATEST NEWS

- Children's Museum and Union Bank Partner up to Bring Jordan a Full Year of "Celebrations"
- Union Bank Sponsors & Participates in the Organizational Success & Excellence Forum
- Union Bank Sponsors Eid Adha Activities of the National Children's Museum

More...

© 2010 Developed by dot.jo. All rights reserved

Exhibit 12

http://www.sgbj.com.jo/sgbj/english/index.asp

The screenshot shows the homepage of SGBJ Internet Banking. At the top left is the SGBJ logo. A banner area contains the text " alt="Click here" border="0" hspace="0" name="bannerad">". To the right is the "Internet Banking" header with navigation links: "> Personalize your site" and "> Search this site". Below this is a search input field and language selection buttons for "عربي" and "English". A navigation bar includes "Your Bank" and "Your Needs" buttons. The main header reads "Welcome to SOCIETE GENERALE DE BANQUE - JORDANIE".

The left sidebar contains several menu sections:

- Your Needs**: Individuals >>, Corporate >>, Private Banking >>, Professionals >>
- Simulator**: Sogecar >>, Sogeloan >>, Sogehome >>, Sogeland >>
- Our Network**: Our branches >>, Our ATMs >>

The main content area features:

- Two cultures' expertise. One Bank.** with an image of a bottle.
- Quotes**: "See the performance of the SGBJ investment products as of July 27th, 2010."
- News**: "Access the news to see SGBJ latest events and new products and services."
- Recruitment**: "Apply for a job or an internship" with the SGBJ logo.
- Links**: A section for external links.

On the right side, there is a "Did you know that our new Branch was inaugurated at Queen Alia International Airport?" notification with a "Did you know?" icon. Below it is a vertical menu with icons for: Legal information, Site Map, Contact us, Webmaster, Claim, and FAQ. Further down are utility links: SGBJ as your home page, Print this page, SGBJ in your favorites, and Refer this site to a friend.

At the bottom, there is a footer with the text "© SGBJ, 2003-2010" and logos for "SOCIETE GENERALE", "SGBL", and "Groupe SGBL".

The bottom-most bar displays financial data: INDEX 2265.4 ▼1.01% Closed, .25 ▲%3.21, APOT 33.00 ▲%0.60, AQRM 0.41 %0.00, ARAI 1.03 ▲%4.04, ARB, and navigation arrows.

Exhibit 13

<http://www.capitalbank.jo/node/147>

كابيتال بنك
Partner with us

Internet Banking

Branch Locator | ATM Locator
Careers | Contact Us | Sitemap | عربي

About Us
Personal Banking
Corporate Banking
SME's
Treasury and Investment
Financial Reports
Latest News

Capital Investments
كابيتال للاستثمارات

National Bank of Iraq

Disclaimer

- Capital Bank will never ask for your User ID and Password.
- You will never receive emails from Capital Bank asking you to log in to your Internet Banking Account.
- Make sure your PC is free of viruses regularly.
- We strongly recommend that you install trusted anti-virus software and firewall on your PC, and that you regularly update them.
- Capital Bank will never ask you for your details or login information via email.
- Select a password that is difficult for others to guess, and change it regularly.
- Your User ID and Password should only be known to yourself. Never disclose them to anyone, or write them in an email.
- Remember to always log out from your account by clicking the 'Logout' tab at the bottom of the page.
- We recommend that you not access the Internet Banking Service from Internet cafes or public places.
- Whenever you log onto the Internet Banking Service site, please verify the last access date and time displayed on the customer information home page.
- When logging onto the Internet Banking Service site, look for the security certificate before entering the User ID and Password. To view the security certificate, click on the 'Lock' icon at the bottom of the page if you are using Internet Explorer.

Accept

Disclaimer

© Copyright Capital Bank, inc 2009. All rights reserved

Exhibit 14



Home Page
About Us
Vision & Mission
Islamic Bank
Educational Corner
Banking Services
Bank Branches
ATMs Locations
Annual Reports
Deposits/ Accounts
Deposits Profits Rates
Careers
Financing Payment Calculation
Contact Us

High 938.9 CHF Low 671.6 High 675 Last update on 2010-08-05

Welcome Aboard..

Your Key to the Islamic Investment

Latest Bank News

Increase Your Savings with the IAB ..

مركز إيداع الأوراق المالية
Securities Depository Center

IslamOnline.net
إسلام أون لاين.نت

Our Services

Visa Card

Shopping..
Visa Electron

Internet Shopping Card

5679595
Phone Banking... Always connected

SMS Service

OWN YOUR HOUSE

Exhibit 15

PRIVACY AND SECURITY STATEMENT

Your Privacy Matters to Us

This section outlines our policy relating to any personal information you might wish to provide us when you visit our site. Your use of our web site indicates your acceptance of our web site Terms of Jordan and this Privacy and Security Statement.

Our business has been built on trust between our customers and ourselves. Unless legally compelled to disclose, we have a commitment to safeguard and keep confidential any information relating to our customers or their financial affairs. Whether it is provided to us in person at one of our branches, over the phone, or while visiting this site, we will strive at all times to ensure that the information is kept confidential and secure.

We may pass information about you and your dealings with us to other HSBC Group Companies or our agents to the extent allowed by law.

All HSBC Group Companies, all our staff and all third parties with permitted access to your information are specifically required to observe our confidentiality obligations.

We will not collect any personal information that identifies a visitor to this site individually unless specified otherwise. Your visit to this site will record only the Domain Name Server part of your e-mail address and of the pages visited. Such information will be used to prepare aggregate information about the number of visitors to the site and general statistics on usage patterns.

Some of this information will be gathered through the use of "cookies". Cookies are small pieces of information that are automatically stored on a person's web browser in their computer that can be retrieved by this site.

You can set your browser to disable persistent cookies and/or session cookies but if you disable session cookies, although you will be able to view our public unsecured website, you will not be able to log onto Internet Banking.

▼ Use of Information and Materials

Products and services referred to in this web site are offered only in jurisdictions where and when they may be lawfully offered by members of the HSBC Group. The materials on these pages are not intended for use by persons located in or resident in jurisdictions that restrict the distribution of such materials by us. Persons accessing these pages are required to inform themselves about and observe any relevant restrictions.

These pages should not be regarded as an offer or solicitation to sell investments or make deposits in any jurisdiction to any person to whom it is unlawful to make such an invitation or solicitation in such jurisdiction.

The information contained in these pages is not intended to provide professional advice or any recommendation and should not be relied upon in that regard. Persons accessing these pages are advised to obtain appropriate professional advice when necessary.

▼ Copyright, Trade Marks

We and other parties own the trade marks, logos and service marks displayed on this site and users are prohibited from using the same without our written permission or of such other parties.

The materials on this site are protected by copyright and no part of such materials may be modified, reproduced, stored in a retrieval system, transmitted (in any form or by any means), copied, distributed, used for creating derivative works or used in any other way for commercial or public purposes without our prior written consent.

▼ No Warranties

While every care has been taken in preparing the information and materials contained in this site, such information and materials are provided to you "as is" without warranty of any kind either express or implied. In particular, no warranty regarding non-infringement, security, accuracy, fitness for a particular purpose or freedom from computer virus is given in conjunction with such information and materials.

▼ E-mail

E-mail messages sent to us over the Internet cannot be guaranteed to be completely secure. We will not be responsible for any damages incurred by users if they send a message to us, or if we send a message to them at their request, over the Internet. We are not responsible in any manner for direct, indirect, special or consequential damages arising out of the use of this web site.

▼ Transmission over the Internet

Due to the nature of the Internet, transactions may be subject to interruption, transmission blackout, delayed transmission and incorrect data transmission. HSBC will not be liable for malfunctions in communications facilities not under our control that may affect the accuracy or timeliness of messages and transactions you send.

▼ Security

We maintain strict security standards and procedures with a view to preventing unauthorised access to your data. We use leading technologies such as (but not limited to) 128 bit verisign secure socket layer data encryption, fire walls and server authentication to protect the security of your data. Access to your account and account information is protected by a password which you set.

Unfortunately, no data transmission over the internet can be guaranteed as totally secure. If your browser is appropriately configured it should tell you whether the information you are sending will be secure (generally by displaying an icon such as a padlock). The combination of a secure browser at your end and our security measures provide you with the best security currently available.

Once we receive your information, we will take all reasonable steps to protect the information. If we no longer need your information, we will destroy or de-identify it.

▼ Cookies

Our public website and Internet Banking services, along with most other major websites, use cookies. Cookies are pieces of information that a website transfers to the cookie file on your computer's hard disk. Cookies enable users to navigate around the website and (where appropriate) enable us to tailor the content to fit the needs of visitors who have accessed the site.

We use two types of cookie on our website.

Session cookies, which are temporary cookies that remain in the cookie file of your computer until you close your browser at which point they are deleted.

Persistent or stored cookies that remain permanently on the cookie file of your computer.

Cookies cannot look into your computer and obtain information about you or your family or read any material kept on your hard drive and, unless you have logged onto Internet Banking, cookies cannot be used to identify who you are.

Cookies cannot be used by anyone else who has access to the computer to find out anything about you, other than the fact that someone using the computer has visited a certain website. Cookies do not in any way compromise the security of Internet Banking.

Cookies will not be used to contact you for marketing purposes other than by means of advertisements offered within our Internet Banking services.

Cookies may be used to record details of pages relating to particular products and services that you have visited on our websites. This is to provide us with generic usage statistics to allow us to improve our websites and to provide you with information about products and services that may interest you. Information on products and services may be provided via the website or by other means.

This does not affect your right to opt-out from receiving marketing material from us.

The web browsers of most computers are initially set up to accept cookies. If you prefer, you can set your web browser to disable cookies or to inform you when a website is attempting to add a cookie. You can also delete cookies that have previously been added to your computer's cookie file.

You can set your browser to disable persistent cookies and/or session cookies but if you disable session cookies, although you will be able to view our public unsecured website, you will not be able to log onto Internet Banking.

If the computer that you are using is set to disable persistent cookies, you will be able to access Internet Banking; however, your navigation of the website may be less enjoyable.

WebTrends

In order to develop our website in line with customer needs HSBC is working with WebTrends to track usage on our website. Webtrends provide HSBC with statistics to show us which pages on our website are visited most frequently and how long visitors spend on our website. We use this information to help us plan how we should improve the website.

WebTrends uses a cookie to track the number of unique users of the site. It basically tells us whether we have a small number of regular visitors to the website or a large number of infrequent visitors. None of the information can be traced to an individual – we do not know who you are as a unique user, merely that there are a certain number of people using the website. The cookie only relates to what goes on in the HSBC website and the information cannot be used for marketing on an individual basis. For more information about how WebTrends collects data, please read their [privacy policy](#).

IMPORTANT: By accessing this web site and any of its pages you are agreeing to the terms set out above.

Exhibit 16

<http://aqaribank.com/FrontEnd/TermsAndCondition.aspx>

نبذة عن البنك | منتجاتنا | فروعنا | خدماتنا | اتصالات | وظائف | أخبار



البنك العقاري المصري العربي
الأمن... اليوم... الغد

شروط وأحكام

مقدمة:

✓ كافة المعلومات والمواد الواردة في هـ البنود والشروط والتفاصيل الواردة تغييرها في اي وقت ودون اشعار.

✓ ان المعلومات الواردة في هذا الموقع لا للارتباط في اي عملية او استشارة ا ضريبة او قانونية الخ ولا ما يجب ا عند اتخاذ اية قرارات بهذا الخصوص وبه عى المشورة اللازمة قبل اتخاذ اي قر

الموافقة المطلقة للحصول على اي مت هذا الموقع لا تتم الا بموافقة البنك العق العربي.

✓ الاستخدام غير مأذون به لمواقع البنك وإن سبيل المثال لا الحصر اي دخول غير مأذ البنك ، او سوء استخدام عبارة الد استخدام اي معلومات معلن عنها في ا محظور نهائياً.

✓ يرجى قراءة هذه الشروط والبنود بعناية عند دخولك الى هذا الموقع أو اي صفحة منه حيث انك ملزم بالتقيد بالبنود أدناه.

✓ في حال عدم موافقتك على هذه الشروط والبنود نرجو عدم الدخول الى هذا الموقع أو الاطلاع على محتوياته أو اي من صفحاته.

✓ جميع حقوق الطبع محفوظة للبنك العقاري المصري العربي.

✓ تعتبر حقوق الطبع في الصفحات وفي شاشات عرض هذه الصفحات وكذلك المعلومات والمواد الواردة في هذه الصفحات والشاشات ملكاً للبنك العقاري المصري العربي.

شروط استخدام المعلومات الواردة في الموقع:

✓ كافة المعلومات والمواد والنصوص وخطوط الربط والرسوم البيانية أو اي بنود اخرى في هذا الموقع

قد تم اعطائها وكما هي موجودة لذلك فإن البنك العقاري المصري العربي لا يضمن دقة هذه المعلومات او ملائمتها للغرض المقصود او اذا كانت هذه المعلومات والمواد واقية ام لا كما ان البنك غير مسؤول صراحة عن اية اخطاء او حذوفات في هذه المعلومات والمواد لا ضمان من اي نوع سواء كان ضمنى او صريح او تشريعى ومما كان نوعه وطبيعته يتعلق بالمعلومات والمواد ويشمل على سبيل المثال لا الحصر الضمانات المتعلقة بعدم انتهاك حقوق الاطراف الاخرى وحق الملكية وامكانية تسويق المعلومات وملائمتها للاستخدام فى اي أغراض اخرى

وخلوها من اية فيروسات.

Exhibit 17

www.rafidain-bank.org

الصفحة الرئيسية
نبذة عن المصرف
المدير العام
أعلان ومناقصات
أخبار الصحف
نشاطات المصرف
إنجازات المصرف
فروعنا
الهيكل التنظيمي
أعضاء مجلس الادارة
نشاطات وحدة الاعلام
المدرء العامين
الاتصال والاستفسار
مواقع تهمك

نظرا لمصادفة أيام عطل خلال
موعد المقابلات تقرر
تزحيف المقابلات لمدة ثلاثة أيام

Exhibit 18

<http://www.standardchartered.com/jo/data-protection-privacy-policy/en/>

The screenshot shows the Standard Chartered Jordan website. At the top left is the Standard Chartered logo and the word "Jordan". To the right are links for "ATMs & Branches", "Investor Relations", "Contact Us", and "Careers", along with a search bar. Below the header is a navigation menu with "Personal Banking", "SME Banking", and "Wholesale Banking" sections. The "Personal Banking" section includes links for "Deposits", "Cards", "Loans", "Investments", "Priority Banking", and "Services". On the left side, there is a "Login" section with options for "Online Banking", "Straight2Bank", and "Remember Selection", a "Login" button, and a link to "Online Security". The main content area features a large blue banner with the text "Data Protection & Privacy Policy" and an image of a family. Below the banner is a breadcrumb trail: "Data Protection & Privacy Policy".

DATA PROTECTION AND PRIVACY STATEMENT

Your Personal Information

This Data Protection and Privacy Statement relates solely to information supplied by you on this Web Site. Standard Chartered Bank, the Data Controller ("SCB") respects the privacy of your personal information and will treat it confidentially and securely.

Any personal information provided by you to SCB through this Web Site will be used for the purpose of providing and operating the products and services you have requested at this Web Site and for other related purposes which may include updating and enhancing SCB's records, understanding your financial needs, conducting credit checks, reviewing credit worthiness and assisting other financial institutions to conduct credit checks, advising you of other products and services which may be of interest to you, for crime/fraud prevention and debt collection purposes, for purposes required by law or regulation, and to plan, conduct and monitor SCB's business. The information collected from you by SCB will be valuable in improving the design and marketing of our range of services and related products for customer use. If you are providing your details in connection with an application for employment, please refer to our "Data Protection and Privacy Statement - Job Applicants" which will be displayed when you apply (see our 'Careers' page). This Policy will not alter or affect any information otherwise provided by you to SCB.

Other than to those individuals and entities listed below your details will not be revealed by SCB to any external body, unless SCB has your permission, or is under either a legal obligation or any other duty to do so. For the purposes detailed above, your information may be disclosed to:

- other Branches or Companies in the SCB Group (ie. SCB, its subsidiaries and affiliates);
- any regulatory, supervisory, governmental or quasi-governmental authority with jurisdiction over SCB Group members;
- any agent, contractor or third party service provider, professional adviser or any other person under a duty of confidentiality to the SCB Group;
- credit reference agencies and, in the event of default, debt collection agencies;
- any actual or potential participant or sub-participant in, assignee, novatee or transferee of, any of the SCB Group's rights and/or obligations in relation to you;
- any financial institution with which SCB has or proposes to have dealings.

The above disclosures may require the transfer of your information to parties located in countries that do not offer the same level of data protection as your home country. However, SCB will ensure that parties to whom your details are transferred treat your information securely and confidentially. SCB also pledges its intention fully to meet any internationally recognised standards of personal data privacy protection and to comply with applicable data protection and privacy laws. We may transfer your information if it is necessary to perform our contract with you and by providing details to SCB via this Web Site you are deemed to consent to any other transfers.

Information held about you is retained as long as the purpose for which the information was collected continues. The information is then destroyed unless its retention is required to satisfy legal, regulatory or accounting requirements or to protect SCB's interests. As a general rule, the maximum retention period is 7 years.

It is your responsibility to maintain the secrecy of any user ID and login password you hold.

Cookies

In order to improve our Internet service to you, we will occasionally use a "cookie" and/or other similar files or programs which may place certain information on your computer's hard drive when you visit an SCB web site. A cookie is a small amount of data that our web server sends to your web browser when you visit certain parts of our site. We may use cookies to:

- allow us to recognise the PC you are using when you return to our web site so that we can understand your interest in our web site and tailor its content and advertisements to match your interests (This type of cookie may be stored permanently on your PC but does not contain any information that can identify you personally.);
- identify you after you have logged in by storing a temporary reference number in the cookie so that our web server can conduct a dialogue with you while simultaneously dealing with other customers. (Your browser keeps this type of cookie until you log off or close down your browser when these types of cookie are normally deleted. No other information is stored in this type of cookie.);
- allow you to carry information across pages of our site and avoid having to re-enter that information;
- allow you access to stored information if you register for any of our on-line services;
- enable us to produce statistical information (anonymous) which helps us to improve the structure and content of our web site;

- enable us to evaluate the effectiveness of our advertising and promotions.

Cookies do not enable us to gather personal information about you unless you give the information to our server. Most Internet browser software allows the blocking of all cookies or enables you to receive a warning before a cookie is stored. For further information, please refer to your Internet browser software instructions or help screen. Alternatively, information on deleting or controlling cookies is available at <http://www.allaboutcookies.org>

Internet Communications

In order to maintain the security of our systems, protect our staff, record transactions, and, in certain circumstances, to prevent and detect crime or unauthorised activities, SCB reserves the right to monitor all internet communications including web and email traffic into and out of its domains.

Your Rights and How to Contact Us

You may have the right under data protection legislation on payment of a fee to request access to personal information about you held by us and to have it corrected where appropriate. If you have that right and you wish to access, correct or delete any of your personal data held by us, or if you have any questions concerning our Data Protection and Privacy Statement please contact the relevant SCB Data Protection representative. You may also have the right to access details held by credit reference agencies and SCB will supply details of the relevant agencies upon request. For the UK please write to: The Regional Head of Legal Compliance UK/Europe, 1 Basinghall Avenue, London EC2V 5DD, England. (Fax number: (+44) (0)20 7885 1871). Other local SCB web sites may have details of local Data Protection Officers.

Contacting You

In providing your telephone, facsimile number, postal and e-mail address or similar details, you agree that SCB may contact you by these methods to keep you informed about SCB products and services or for any other reason. If you prefer not to be kept informed of SCB products and services, please contact SCB by [E-mail](#).


SCB reserves the right to amend its prevailing Data Protection and Privacy Statement at any time and will place any such amendments on this Web Site. This Data Protection and Privacy Statement is not intended to, nor does it, create any contractual rights whatsoever or any other legal rights, nor does it create any obligations on SCB in respect of any other party or on behalf of any party.

COPYRIGHT © STANDARD CHARTERED PLC 2006. ALL RIGHTS RESERVED.



Exhibit 19

http://www.nbk.com/Privacy_en_gb.aspx



الوطني
NBK

[Home](#) | [Contact Us](#) | [عربي](#)

Privacy Statement

NBK.com has created this privacy statement in order to demonstrate our firm commitment to privacy. We shall never sell your personal information to other companies for their independent marketing purposes. We maintain physical, electronic and procedural safeguards to prevent unauthorized access to your personal information and to protect you against the criminal misuse of that information. We restrict access to your account(s) to only those employees involved in providing the services you've requested.

The following discloses our information gathering and dissemination practices for the NBK.com website.

IP Address and Cookies

Your IP address may be used to gather broad demographic information. In order to provide better service, we may use "cookies". Our site may use cookies for administrative purposes and to enhance your online experience by keeping track of your behavior within the site and to make sure you do not see the same special offers repeatedly.

Your contact information may be used by NBK to contact the you when necessary. Users may opt-out of receiving future mailings; see the Choice section below.

Links to Third Party Sites


This site contains links to other sites. Third party web sites have different privacy policies and/or security standards governing their sites, we advise you to review the privacy policies and terms and conditions of these sites prior to providing any personal information. Links to non-NBK web sites are provided solely for information purposes. If you choose to access such sites NBK.com is not responsible for the privacy practices or the content of such sites.

Security

While we have security measures in place to protect the loss, misuse and alteration of the information under our control and while we have appropriate firewalls in place to block unauthorized access to any user data stored on our servers, we shall not be responsible for any loss, misuse, alternation, or unauthorized access to any such information or data.

Children's Guidelines

This site is not intended to be used by children.



Best Bank in
The Middle
East Award
[View Awards →](#)

Choice

When we request information about you, you are given the choice not to receive communications from our partners. You may remove your information from our database; choose not to receive future communications, or terminate any of our services.

If you have any questions about this privacy statement or the practices of this site, please contact webmaster@nbk.com

Special Offers and Promotions

Transactions and dealings you enter into with any merchant in respect of any of the special offers and promotions offered on NBK.com shall be effective only between you and the merchant, and NBK shall neither be a party thereto nor be responsible for any such transaction.. National Bank of Kuwait hereby disclaims any warranty, express or implied, connected with any of the content displayed on nbk.com or the information provided by the merchants and/or third parties.

National Bank of Kuwait

NBK.com welcomes your feedback and comments in order to provide its customers with better service.

For any questions or information related to NBK.com third party products, please contact the responsible merchant who holds full responsibility.

Exhibit 20

<http://www.blombank.com/English/AbroadBranchesPage.aspx?pageid=9026&CountryID=9269>

The screenshot displays the BLOM Bank SAL website. At the top left is the BLOM BANK logo with the tagline "Peace of Mind". To the right are navigation links: العربية العربية | Careers | Sitemap | Contact Us, followed by a search bar labeled "Keywords" and a "Go" button. Below this is a main navigation menu with links: About Us, The Group, Network, Products & Services, Investor Relations, Delivery Channels, and News & Publications. A secondary menu lists: Retail Banking | Corporate Banking | Private & Investment Banking | Insurance Services | Islamic Banking. A "SIGN UP FOR UPDATES" section includes an email input field and a "Submit" button. A "DELIVERY CHANNELS" section lists: Internet Banking, Branches, ATMs, SMS Alerts, Call Center, and Allo BLOM. The main content area features a large image of a modern building at night with the text "BLOM Bank SAL". Below the image is a breadcrumb trail: Home / Network / BLOM Bank SAL, and utility links: Send this page, Print, Text: T | I. A sidebar menu on the left shows: BLOM Bank SAL, BLOM Bank SAL, Branches, Branches Abroad & Representative Office, and Entities Branches. To the right of this menu is the BLOM BANK logo with "JORDAN" and "Jordan" text below it. At the bottom, a horizontal line contains a list of countries: Lebanon • Cyprus • Jordan • France • UAE • United Kingdom • Romania • Switzerland • Syria • Egypt. Below this line is the copyright notice: Copyright 2009 BLOM BANK. All rights reserved.

Appendix D

**DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND
OF THE COUNCIL**

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-

border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect

on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of

State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially

in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services

competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of

implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing for which the data are intended;
- (c) any further information such as
 - the recipients or categories of recipients of the data,
 - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
 - the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing;
- (c) any further information such as
 - the categories of data concerned,
 - the recipients or categories of recipients,
 - the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort

or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him

and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to

consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

- (a) the name and address of the controller and of his representative, if any;
- (b) the purpose or purposes of the processing;
- (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- (d) the recipients or categories of recipient to whom the data might be disclosed;
- (e) proposed transfers of data to third countries;
- (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.
2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, *inter alia* before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals,

the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in

Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p. 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.